P3NK-E082-04

NetVehicle 取扱説明書



NetVehicle-L10

FUJITSU



はじめに

このたびは、NetVehicle-L10 をお買い上げいただき、まことにありがとうございます。
NetVehicle-L10（以降 NetVehicle と略します）は、LAN 間通信を行うための小型ルータです。
NetVehicle では WWW ブラウザを使用して、各種設定を簡単に行うことができます。また、設定画面は WWWのホームページと同じハイパーテキスト形式になっているので､設定方法や設定項目の説明をクリックひとつで参照できます。インターネットや LAN をさらに活用するために、NetVehicle をご利用ください。

2002 年 8 月

目　次



コピーライトについて

本製品には、カルフォルニア大学およびそのコントリビュータによって開発され、下記の使用条件とともに配付されている FreeBSD の一部が含まれています。

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase "this text" refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase "This material" refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

本製品には、WIDEのKAMEプロジェクトによって開発され、下記の使用条件とともに配布されているソフトウェアが含まれています。



安全上のご注意

警告表示について

取扱説明書では、使用者および周囲の方々や財産に損害を与えないための警告表示をしています。警告表示は、警告レベルの記号と警告文の組み合わせになっています。

⚠警告　正しく使用しない場合、死亡または重傷のおそれがあることを示します。

⚠注意　正しく使用しない場合、軽傷または中程度の傷害を負うおそれがあることを示します。
また、当該製品自体もしくは他の使用者の財産に対して損害を与えるおそれがあることを示します。

⚠警告　本装置を安全にお使いいただくために、必ずお守りください。正しく使用しない場合、死亡または重傷のおそれがあることを示します。

作業区分	警告事項
感電・火災について	本装置の分解・解体・改造・再生を行わないでください。 また、本装置の上には絶対に物をのせないでください。感電・火災・故障の原因となります。
	直射日光の当たる場所や暖房機の近く、湿気、ホコリの多い場所には置かないでください。 感電や火災のおそれがあります。
	通気孔がある機種の場合、装置内部が高温になるため通気孔をふさがないでください。火災のおそれがあります。
	万一装置から発熱・発煙・異臭が発生したときは、「｜／○」スイッチ（電源スイッチ）を「○」側へ押して、電源を切断してください。 電源を切断したら、富士通の技術員に連絡してください。そのまま使用すると、感電や火災のおそれがあります。なお、この場合、通信中のデータは保証されません。
	感電のおそれがあります。必ずアース線を接続してください。 アース接続は、必ず電源プラグをコンセントに接続する前に行ってください。 アース接続を外すときには、必ず電源プラグをコンセントから抜いてから行ってください。
	異常発生時には、直ちに電源プラグをコンセントから抜いてください。 アース線は電源プラグを抜くまで外さないでください。
	電源ケーブルを傷つけたり、加工したりしないでください。 電源ケーブルの上に物をのせたり、絡みつけたり、足を引っかけたりしないようにしてください。 感電や火災のおそれがあります。その他のケーブル類も同様です。
	本装置の電源ケーブルは、タコ足配線にしないでください。 コンセントが過熱し、火災の原因となることがあります。
	電源プラグの金属部分、およびその周辺にほこりが付着している場合は、乾いた布でよく拭き取ってください。 そのまま使用すると、火災の原因になります。
	電源ケーブルは、プラグ部分をもってコンセントから抜いてください。 プラグが傷んで感電や火災のおそれがあります。
	電源プラグは、電源コンセントに確実に奥まで差し込んでください。 差し込みが不十分な場合、感電・発煙・火災の原因となります。
	ぬれた手で電源プラグを抜き差ししないでください。感電のおそれがあります。
	電源ケーブルや電源プラグが傷んだり、コンセントの差し込み口がゆるいときは使用しないでください。 そのまま使用すると、感電・火災の原因となります。
	使用中の装置を布でおおったり、包んだりしないでください。熱がこもり、火災の原因となることがあります。
	電源ケーブルを束ねて使用しないでください。発熱して、火災の原因となることがあります。
	雷が鳴りだしたら、電源ケーブルやケーブル類に触れないでください。感電の原因となります。

作業区分	警告事項
感電・火災について	コーヒーなどの液体やクリップなどの金属片が装置内部に入らないように気をつけてください。また、装置内部に異物が入るのを防ぐため、装置の上には物を置かないでください。感電や火災のおそれがあります。 モジュラージャックには指などを入れないでください。感電の原因となります。
破損・負傷について	本装置を縦置きおよび多段積みで使用しないでください。 装置が破損したり、作業者が負傷したりするおそれがあります。
	振動の激しい場所や傾いた場所など、不安定な場所に置かないでください。 落下したりして、けがの原因となることがあります。
	装置の上に物を置いたり、装置の上で作業したりしないでください。 装置が破損したり、作業者が負傷したりするおそれがあります。
	梱包に使用しているビニール袋は、お子様が口に入れたり、かぶって遊んだりしないよう、ご注意ください。 窒息の原因となります。
	本装置を廃棄するときは、他のゴミと一緒に捨てないでください。火中に投じると破裂するおそれがあります。

⚠注意　正しく使用しない場合、軽傷または中程度の傷害を負うおそれがあることを示します。また、当該製品自体もしくは他の使用者の財産に対して損害を与えるおそれがあることを示します。

作業区分	警告事項
故障について	本装置を縦置きおよび多段積みで使用しないでください。故障の原因となります。
	振動の激しい場所や傾いた場所など、不安定な場所に置かないでください。故障の原因となります。
	装置の上に物を置いたり、装置の上で作業したりしないでください。故障の原因となります。
	本装置は、屋内に設置してください。屋外で使用すると故障の原因となります。
	極端な高温、あるいは低温状態や温度変化の激しい場所で使用しないでください。故障の原因となります。
	塩害地域では使用しないでください。故障の原因となります。
	衝撃や振動の加わる場所で使用しないでください。故障の原因となります。
	薬品の噴囲気中や、薬品にふれる場所で使用しないでください。故障の原因となります。
	電子レンジなど、強い磁界を発生する装置のそばで使用しないでください。故障の原因となります。
	本装置を並べて使用する場合、側面に 3cm 以上の間隔をあけてください。故障の原因となります。
	国内でのみ使用してください。本装置は国内仕様になっているので、海外ではご使用になれません。
	内部に液体や金属類などの異物が入った状態で使用しないでください。故障の原因となります。
	本装置を移動するときは、必ず電源ケーブルを抜いてください。故障の原因となります。
電波障害について	ラジオやテレビジョン受信機のそばで使用しないでください。 ラジオやテレビジョン受信機に雑音が入る場合があります。
感電について	感電するおそれがありますのでサービスマン以外はカバーを開けないでください。 また、保守時には必ず電源ケーブルを抜いてください。

メンテナンスに関するご注意

- 決してご自身では修理を行わないでください。故障の際は、富士通の技術員または富士通が認定した技術員によるメンテナンスを受けてください。
- 本装置をご自身で分解したり改造したりしないでください。本装置の内部には、高電圧の部分および高温の部分があり危険です。

警告ラベルについて

本装置の底面には以下の内容の警告ラベルが貼りつけられています。警告ラベルは絶対にはがさないでください。また、本ラベルが汚染、磨耗などにより確認できなくなった場合には、購入元に連絡し、貼り替えてください。

	⚠警告
感 電	感電のおそれがあります。必ずアースを接続してください。アース接続は、必ず電源プラグをコンセントに接続する前に行ってください。アース接続を外すときには、必ず電源プラグをコンセントから抜いてから行ってください。
	⚠警告
感 電	異常発生時には、直ちに電源プラグをコンセントから抜いてください。 アース線は電源プラグを抜くまで外さないでください。
	⚠注意
感 電	感電するおそれがありますのでサービスマン以外はカバーを開けないで下さい。 また、保守時には必ず電源コードを抜いてください。

使用上のご注意

- 本製品として提供される取扱説明書、装置本体およびファームウェアは、お客様の責任においてご使用ください。
- 本製品の使用によって発生する損失やデータの損失については、富士通株式会社では一切責任を負いかねます。また、本製品の障害の保証範囲はいかなる場合も、本製品の代金としてお支払いいただいた金額を超えることはありません。あらかじめご了承ください。
- 本製品にて提供されるファームウェアおよび本製品用として富士通株式会社より提供される更新用ファームウェアを、本製品に組み込んで使用する以外の方法で使用すること、また、改変や分解を行うことは一切許可しておりません。

ファームウェアの更新について

NetVehicle本体で使用するファームウェアは定期的に更新されます。最新の機能をご利用になりたい場合はftpを使ってインターネット経由でご利用のファームウェアをダウンロードしてください。更新方法については「メンテナンスメニューを使う（P.116）」を参照してください。
なお、ファームウェアを更新した場合、操作方法などが本書の内容と一部異なる場合があります。このような場合は、富士通の NetVehicle のサポートページで最新の情報を確認してください。
http://telecom.fujitsu.com/jp/products/telcom/nv/

セキュリティの確保について

管理者パスワードを設定しない場合、ネットワーク上の誰からでも NetVehicle の設定を行うことができます。セキュリティの面からは非常に危険なため、管理者パスワードを設定することを強く推奨します。

電波障害自主規制について

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

ハイセイフティについて

本製品は、一般事務用、パーソナル用、家庭用、通常の産業用等の一般的用途を想定して設計・製造されているものであり、原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療用機器、兵器システムにおけるミサイル発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途（以下「ハイセイフティ用途という」）に使用されるよう設計・製造されたものではございません。お客様は、当該ハイセイフティ用途に要する安全性を確保する措置を施すことなく、本製品を使用しないでください。ハイセイフティ用途に使用される場合は、NetVehicleサポートセンターまでご相談ください。



本書の構成と使いかた

本書では、NetVehicle で基本的な操作を行うための環境を整えるまでの手順を説明しています。また、インターネットやネットワーク間接続をするための基本的な設定方法も説明します。
なお、NetVehicleのトップページと本書の記載内容とが異なる場合は、各ページの指示に従って設定を行ってください。
また、NetVehicleのトップページから富士通のNetVehicleのサポートページをワンタッチで参照できます。より高度な使い方や、本書に掲載されている以外の各種設定例、機能追加などは、NetVehicleのサポートページを参照してください。NetVehicle に関する最新の情報を入手できます。

各章の役割

本書の構成は次のようになっています。

「第 1 章　お使いになる前に」
NetVehicle を使う前に必要な準備などを説明します。

「第 2 章　NetVehicle を設定するまで」
NetVehicle とパソコンをつないで設定を行い、LAN に接続するまでを説明します。

「第 3 章　NetVehicle で CATV インターネット接続する」
NetVehicle でインターネット接続するための設定方法を説明します。

「第 4 章　NetVehicle でネットワーク間接続する」
NetVehicle のネットワーク間接続するための設定方法を説明します。

「第 5 章　NetVehicle の便利な機能を活用する」
NetVehicle の便利な機能の活用方法について説明します。

「第 6 章　運用管理とメンテナンス」
NetVehicle の運用管理や確認を行う方法を説明します。

「第 7 章　困ったときには」
通信ができなくなった場合や、使用中のトラブルの対処方法を説明します。

「付録」
本書で使われている用語や、NetVehicle の仕様などを説明します。

本書の使いかた

本書で使用しているマーク類は、次のような内容を表しています。

 NetVehicle をお使いになるうえで役に立つ知識を、コラム形式で説明しています。

 こんな事に気をつけて
NetVehicle をご使用になる際に、注意していただきたいことを説明しています。

 操作手順で説明しているものの他に、補足情報を説明しています。

 操作方法など関連事項を説明している箇所を示します。

 製造物責任法（PL）関連の警告事項をあらわしています。NetVehicleをお使いの際は必ず守ってください。

 製造物責任法（PL）関連の注意事項をあらわしています。NetVehicleをお使いの際は必ず守ってください。

本書における商標の表記について

Microsoft、Windows および WindowsNT は、米国 Microsoft Corporation の米国およびその他における登録商標です。

Macintosh は、アップルコンピュータ社の商標です。

Adobe、Adobe ロゴ、Adobe Acrobat、Adobe Acrobat ロゴは、Adobe Systems Incorporated（アドビシステムズ社）の商標です。

Netscape Communications、Netscape Communications logo、Netscape Navigator、Netscape は、米国 Netscape Communications Corporations の登録商標です。

AMD、AMD 社ロゴマーク、ならびにその組み合わせは、Advanced Micro Devices, Inc. の商標です。
Magic Packet、PCnet は Advanced Micro Devices, Inc. の商標です。
AMD and the AMD Logo are registred trademarkes and Magic Packet and PCnet are trademarkes of Advanced Micro Devices, Inc.

本書に記載されているその他の会社名および製品名は、各社の商標または商標です。
なお、本文中では® および™ マークは省略しています。
Windows® Me の正式名称は、Microsoft® Windows® Millennium Edition operating system です。
Windows® 98 の正式名称は、Microsoft® Windows® 98 operating system です。
Windows® 95 の正式名称は、Microsoft® Windows® 95 operating system です。
Windows® 2000 の正式名称は、Microsoft® Windows® 2000 operating system です。
WindowsNT® 4.0 の正式名称は、Microsoft® WindowsNT® Server network operating system Version 4.0、または Microsoft® WindowsNT® Workstation operating system Version 4.0 です。
WindowsNT® 3.51 の正式名称は、Microsoft® WindowsNT® Server network operating system Version 3.51、または Microsoft® WindowsNT® Workstation operating system Version 3.51 です。

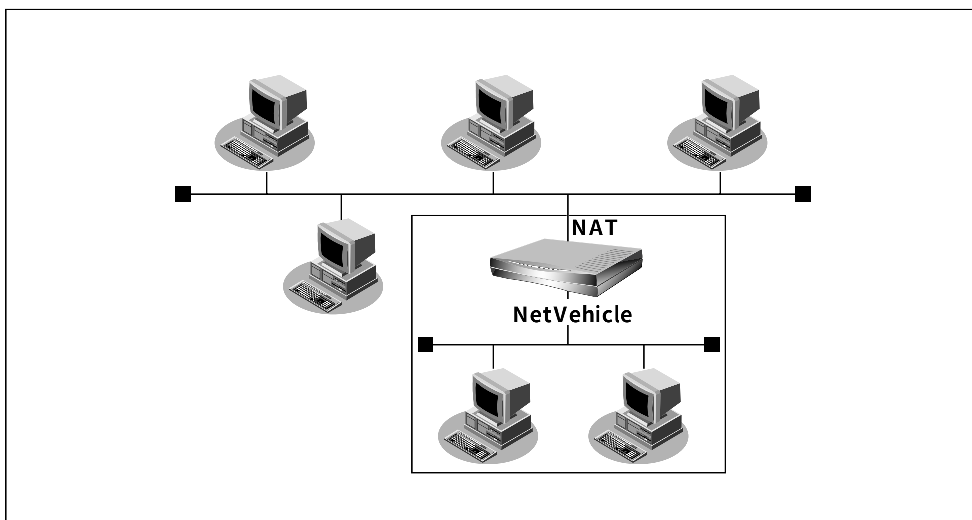


NetVehicle でできること

NetVehicle は 2 つの LAN インタフェース（LAN0/LAN1）を持つ LAN 間ルータです。

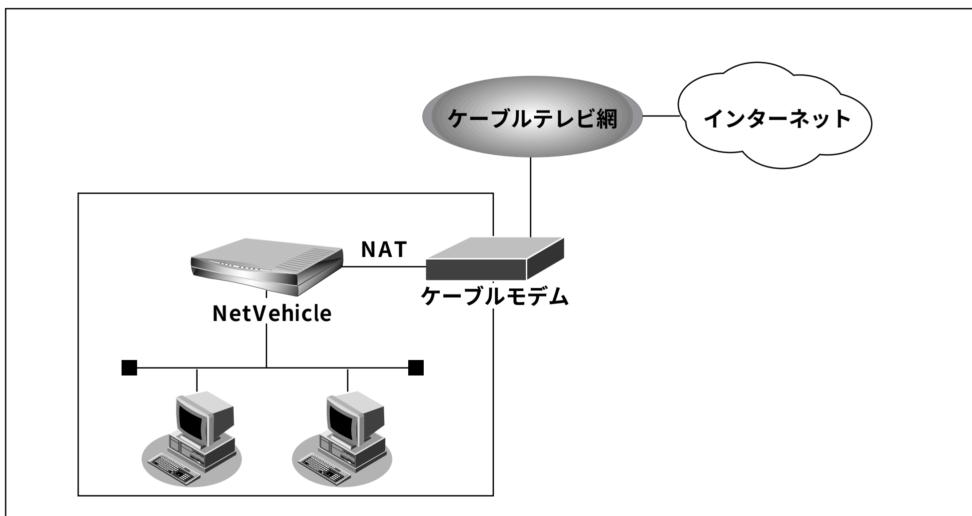
●かんたんに LAN を構築できる

お使いの LAN に、NAT/DHCP を使用してプライベートな LAN を手軽に追加できます。
ご購入時の状態の NetVehicle では、LAN につないだあと、電源を入れるだけで通信できます。（P.50）



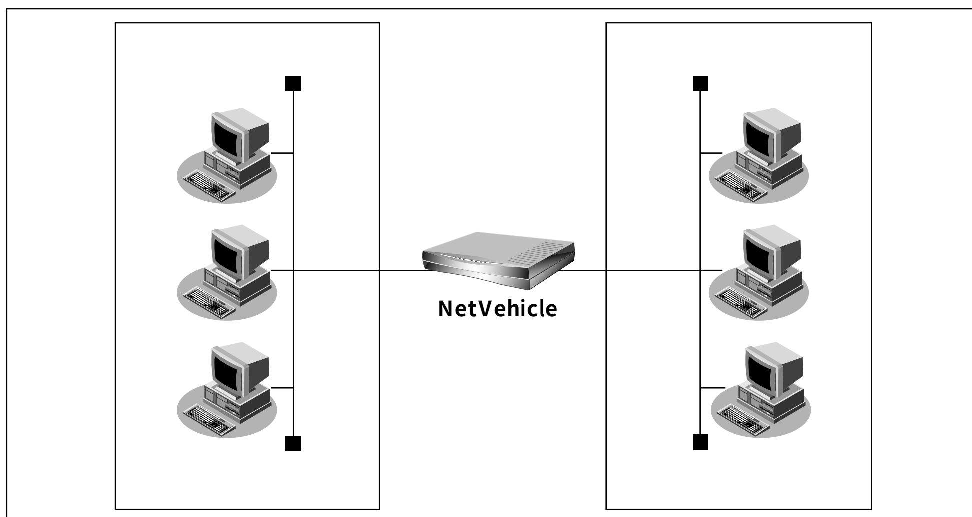
●インターネットへ「かんたん」「高速」にアクセスできる

CATV 回線を利用して複数台のパソコンをインターネットに接続できます。
CATV 利用者間のセキュリティも万全です。（P.44）



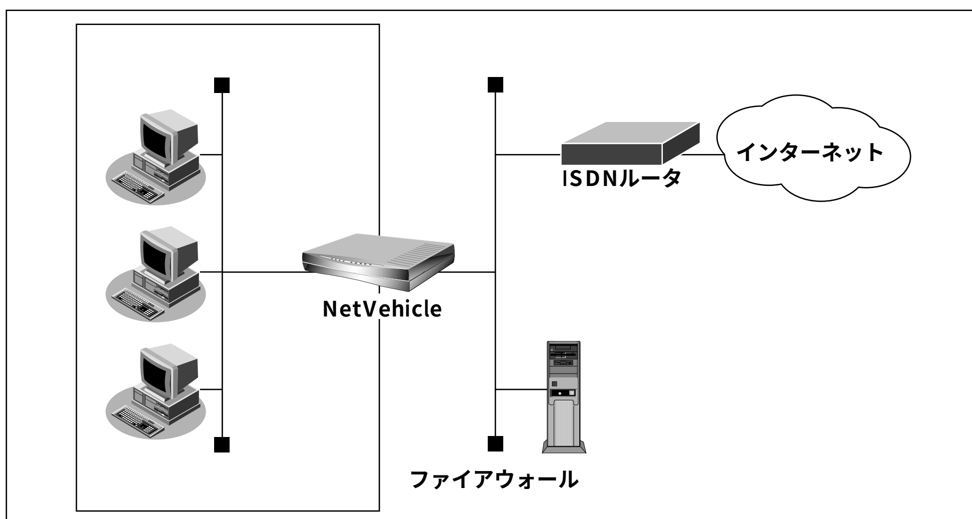
●かんたんにLANを分割できる

LANどうしの接続や分割がかんたんにできます。
ご購入時の状態のNetVehicleでは、LANにつないだあと、基本設定を選択するだけでかんたんに通信できます。（P.52）



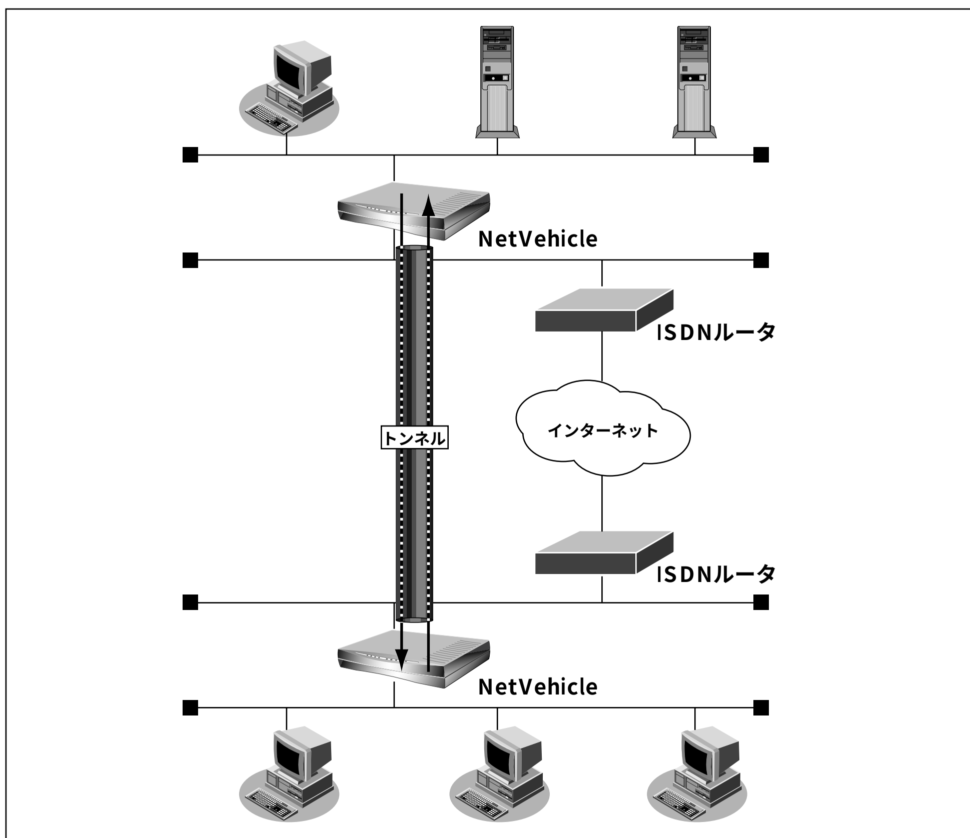
●かんたんにファイアウォールを構築できる

外部からの不正なアクセスも遮断できます。



●かんたんにVPNを構築できる

インターネットにつながっているLANどうしをかんたんにVPNで接続できます。（P.104）



●かんたんな操作で多彩なサポート機能を使用できる

- WWWブラウザを使ってかんたんに設定できます。
- DNS機能やDHCP機能など便利な機能をサポートしています。
- スケジュール機能を使ってパソコンを自動的に起動できます。
- 通信状況のチェックがかんたんです。
- ファームウェアの更新がかんたんです。



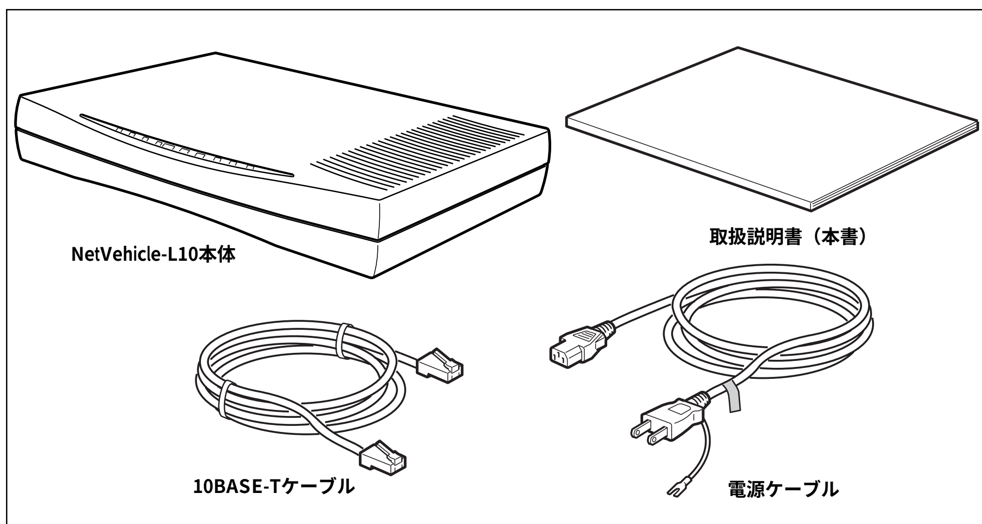
お使いになる前に

この章では、
NetVehicle を使う前に必要な準備などを説明します。



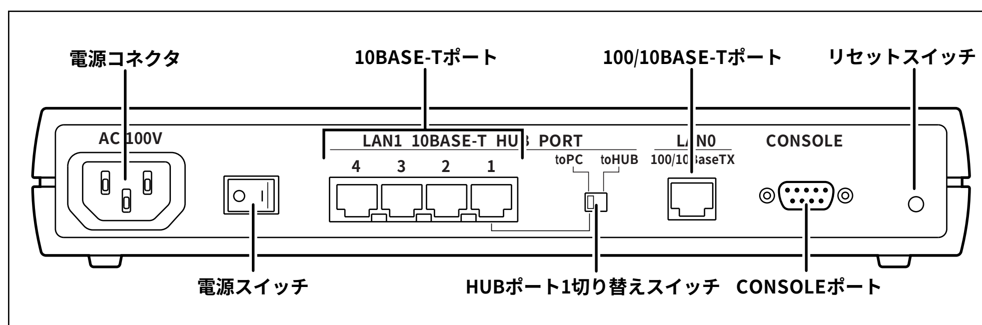
梱包内容／各部の名称と働きを確認する

NetVehicleをお使いになる前に、梱包内容を確認してください。NetVehicleのパッケージには、以下のものが同梱されています。すべてそろっていることを確認してください。
もし、足りないものがあったり、取扱説明書に乱丁、落丁などがありましたら購入元へご連絡ください。



- 電源ケーブル　　NetVehicleとコンセントをつなぎます。
- 10BASE-Tケーブル　　NetVehicleをパソコンまたはハブにつなぐためのケーブルです。両端に８ピンのモジュラプラグがついています。

NetVehicle背面

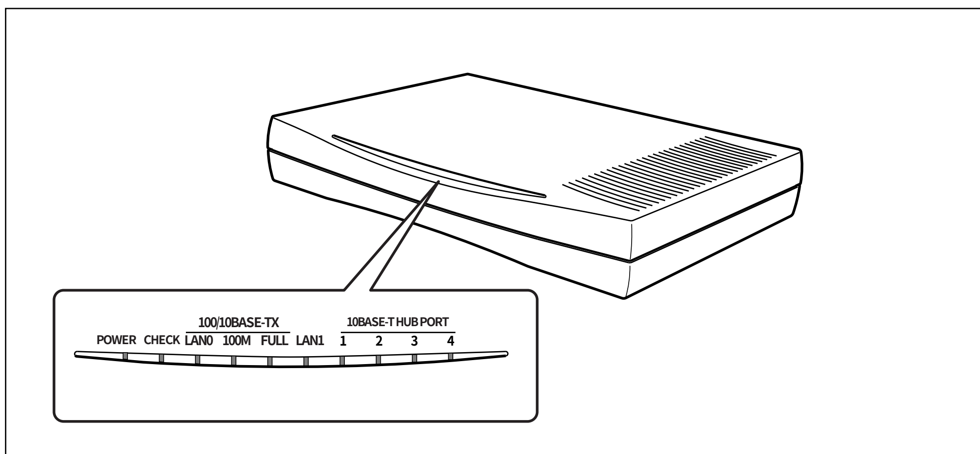


- 電源コネクタ　　付属の電源ケーブルの先をここに差し込みます。
- 電源スイッチ　　「｜」側へ押すと、電源が入ります。
  「○」側へ押すと、電源が切れます。
- 10BASE-Tポート　　NetVehicleをパソコンやワークステーションとつなぐときに使います。
- HUBポート１切り替えスイッチ
  HUBポート１を切り替えるときに使います。
  ・toPC側に切り替えるとパソコンにつなぐことができます。
  ・toHUB側に切り替えるとハブにつなぐことができます。
- 100/10BASE-Tポート　　10Mbpsまたは100MbpsのHUB装置とつなぐときに使います。
  100BASE-TXと10BASE-Tの切り替えは自動的に行います。
- CONSOLEポート　　コンソール用のポートです。RS232Cケーブルでパソコンを接続できます。
- リセットスイッチ　　装置の再起動を行います。



表示ランプの意味

NetVehicleの前面には10個のランプがあります。動作状況により緑色またはオレンジ色で点灯／点滅します。電源を入れていない状態ではランプは消灯しています。



正常に動作しているとき

- POWERランプ　電源の状態を示します。電源を入れると緑色で点灯し、切断すると消灯します。
- LAN0ランプ　LAN0側の状態を表示します。通信可能な状態で緑色で点灯し、通信が行われている（データがやり取りされている）間は緑色で点滅します。ケーブルが抜けている場合は、オレンジ色で点滅します。
- 100Mランプ　100Mbpsで通信中の場合は、緑色で点灯し、10Mbpsで通信中の場合は、ランプが消灯します。
- FULLランプ　全二重通信の場合は緑色で点灯し、半二重通信の場合はランプが消灯します。
- LAN1ランプ　LAN1側の状態を表示します。通信可能な状態で緑色で点灯し、通信が行われている（データがやり取りされている）間は緑色で点滅します。
- HUB PORTランプ　10BASE-Tポート（1～4）の状態を表示します。ポートにパソコンを接続しているとき、緑色で点灯します。NetVehicleがデータを受信している間は緑色で点滅します。

動作が異常なとき

- CHECKランプ　エラー発生時に、オレンジ色で点灯します。

NetVehicle本体の電源異常を検出したとき

すべてのランプが消灯します。このような場合には、すぐに電源スイッチを「○」側へ押してください。

表示ランプ詳細

●通常時

		POWER	CHECK	LAN0	100M	FULL	LAN1	HUB PORT 1～4
		電源状態表示	システム状態表示	LAN状態表示	100M/10M	FULL/HALF	LAN状態表示	10BASE-T HUBの1～4の状態表示
LEDの表示	緑点灯	ON	—	リンク確立	100M	全二重	リンク確立	ポートに機器が接続している
	緑点滅	—	—	通信中	—	—	通信中	ポートで受信中（データ）
	消灯	OFF	—	—	10M	半二重	正常	ポート未接続
	橙点滅	—	—	異常	—	—	異常	—
	橙点灯	—	異常	—	—	—	—	—

●ファームウェア更新時

	POWER	CHECK	LAN0	100M	FULL	LAN1
ファーム消去	緑点灯	緑点滅	消灯	消灯	消灯	消灯
ファーム更新中（0～50%）	緑点灯	緑点滅	緑点滅	消灯	消灯	消灯
ファーム更新中（51～100%）	緑点灯	緑点滅	緑点滅	緑点滅	消灯	消灯
再起動待ち状態	緑点灯	緑点滅	緑点滅	緑点滅	緑点滅	消灯



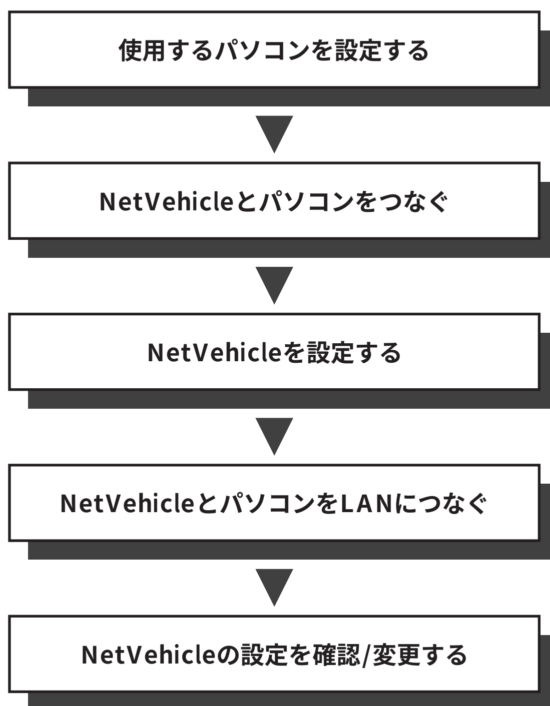
NetVehicleを接続するまで

この章では、
パソコンの準備、NetVehicleの設定方法、LANへの接続方法について説明します。



NetVehicleをLANに接続するまで

NetVehicle を設定し、LAN に接続するまでには以下の作業が必要です。
お使いになるネットワーク上に DHCP サーバがある場合、NetVehicle がご購入時の状態では、お使いになるネットワークに接続するだけでプライベート LAN を構築できます。





お使いになるネットワークを確認する

NetVehicle を使って LAN を構築する前に、お使いになるネットワーク上のホストの IP アドレスおよび DHCP サーバの有無を確認してください。

ネットワーク上のホストの IP アドレス

TCP/IP では、ネットワーク上の各コンピュータ（慣例的にホストといいます）の IP アドレスと NetVehicle の IP アドレス（ご購入時には、LAN0 側：192.168.0.1、LAN1 側：192.168.1.1 に設定）が重複すると、ホストと NetVehicle 間の通信ができなくなります。ネットワーク上に「192.168.0.1」または「192.168.1.1」という IP アドレスを持つホストが存在する場合は、NetVehicle の IP アドレスを変更する必要があります。


IP アドレスの変更→「「かんたん設定」で設定する」（P.50）、「「詳細設定」で設定する」（P.57）

各ホストの IP アドレスなどを静的に割り当てる場合は、この重複が発生しないように注意してください。動的割り当てを行っている場合でも、DHCP サーバが割り当てる IP アドレスと NetVehicle の IP アドレスが重複しないように設定を変更する必要があります。また、ブロードキャストアドレスは設定できません。


使ってはいけない IP アドレス、ブロードキャストアドレス→「Q&A　Q19」（P.147）



◆ TCP/IP によるネットワークでは、各ホストを識別するため、「IP アドレス」などの割り当てが必要です。

インターネットなどでたびたび出てくる「IP アドレス」は「ネットワーク部」と「ホスト部」の 2 つの要素から成り立っています。例えば「192.168.1.10」という IP アドレスの場合なら、最初の「192.168.1.」までを「ネットワーク部」といい、最後の「10」を「ホスト部」といいます（クラス C の場合）。
ネットワーク部が同じ IP アドレスを持つホストは、同じネットワーク上にあると認識されます。さらに、ホスト部によって同一ネットワーク上の各ホストが識別されます。
このため、「IP アドレス」を各ホストに割り当てるときは、以下のことを考慮しなければなりません。
・同一ネットワークに含めるホストに対して、同じネットワーク部を与えなければならない。
・同一ネットワーク内では、ホスト部を重複させてはいけない。

DHCP サーバの有無

ネットワーク上の各ホストへの IP アドレスの割り当てを、DHCP サーバで行っているか確認します。NetVehicle と同一のネットワーク上に DHCP サーバがある場合は、NetVehicle の DHCP サーバ機能を使用しないよう設定を変更する必要があります。


DHCP サーバ機能の設定→「DHCP サーバ機能」（P.84）



◆ DHCP サーバの使用で IP アドレスを自動割り当て

以前はネットワーク管理者が手動で IP アドレスを割り当てていましたが、IP アドレスの重複を避けたり、パソコンの台数が増えるたびに設定を行う必要があり、大変手間がかかっていました。このような割り当てかたを「IP アドレスなどの静的割り当て」といいます。

のちに、使用する IP アドレスの範囲をあらかじめ指定しておき、ネットワーク上でパソコンを起動するたびに順次アドレスを割り当てるしくみが考案されました。このようなアドレスの割り当てかたを「IP アドレスなどの動的割り当て」といい、「DHCP（Dynamic Host Configration Protocol）」というプロトコルを使用します。DHCP の使用により、ネットワーク管理にともなう負担が軽減されます。



使用するパソコンを設定する

LAN カードを用意する

お使いのパソコンに Ethernet ポートがあることを確認してください。
Ethernetポートがないパソコンの場合は、LANカードを取り付ける必要があります。パソコンやLANカードに添付のマニュアルに従って正しく設定をしてください。

TCP/IP プロトコルを利用できるようにする

NetVehicleを使うには、パソコンに「TCP/IP」というネットワークプロトコルモジュールをインストールしておく必要があります。また、実際に通信するためには、パソコン側で以下の設定が必要です。

- IP アドレス
- ネットマスク
- DNS サーバアドレス
- デフォルトゲートウェイ
- ドメイン名

なお、NetVehicle にこれらの設定を自動的に行わせることもできます。



◆「TCP/IP」って何？
インターネットで利用されている標準の通信規約（プロトコル）をまとめて、TCP/IP と呼びます。

パソコンの設定（Windows® 98）

パソコンに TCP/IP がインストールされていることを確認します。
Windows® 95 をお使いの場合は、Windows® 95 のマニュアルを参照してください。
Windows デスクトップの設定で「Webスタイル」を指定してある場合は、「ダブルクリック」と記載してあるところは「シングルクリック」で操作できます。

1. [コントロールパネル] ウィンドウを開き、[ネットワーク] アイコンをダブルクリックします。

2. [ネットワーク] ウィンドウで [ネットワークの設定] タブをクリックして選択します。

「現在のネットワークコンポーネント」一覧に「TCP/IP」または「TCP/IP→□□□（すでにダイヤルアップの設定を行っている場合は□□□内にお使いの LAN カードの名称が表示されます）」があることを確認します。

補足　一覧に TCP/IP が見つからない場合は、TCP/IP のインストールが必要です。Windows® 98 のマニュアルを参照して、インストールしてください。

3. 一覧から「TCP/IP」または「TCP/IP→□□□（□□□内はお使いのLANカードの名称）」をクリックして選択します。



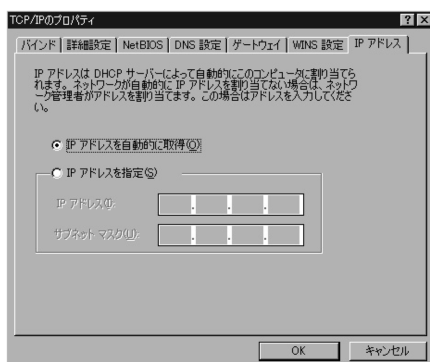

こんな事に気をつけて

「TCP/IP →ダイヤルアップアダプタ」を選択しないでください。

4. ［プロパティ］ボタンをクリックします。

［TCP/IP のプロパティ］画面が表示されます。

5. ［IP アドレス］タブ画面で「IP アドレスを自動的に取得」を選択します。





「DHCP サーバ機能」を使用しない→「Q & A Q15」（P.144）

6. ［OK］ボタンをクリックします。

［ネットワーク］ウィンドウに戻ります。

7. ［OK］ボタンをクリックします。

パソコンを再起動するかを確認するメッセージが表示されます。

8. ［はい］ボタンをクリックし、パソコンを再起動します。

設定した内容は、再起動後に有効になります。

パソコンの設定（WindowsNT® 4.0）

パソコンに TCP/IP がインストールされていることを確認します。
WindowsNT® 3.51 をお使いの場合は、WindowsNT® 3.51 のマニュアルを参照してください。
Windows デスクトップの設定で「Web スタイル」を指定してある場合は、「ダブルクリック」と記載してあるところは「シングルクリック」で操作できます。

1. **［コントロールパネル］ウィンドウを開き、［ネットワーク］アイコンをダブルクリックします。**

2. **［ネットワーク］ウィンドウで［プロトコル］タブをクリックして選択します。**



3. **「ネットワークプロトコル」一覧に TCP/IP プロトコルが含まれていることを確認します。**

補足 一覧に TCP/IP プロトコルが見つからない場合は、TCP/IP のインストールが必要です。WindowsNT® 4.0 のマニュアルを参照して、インストールしてください。

4. **一覧から「TCP/IP プロトコル」をクリックして選択します。**

5. **［プロパティ］ボタンをクリックします。**
［Microsoft TCP/IP のプロパティ］画面が表示されます。

6. **［アダプタ］のプルダウンメニューから、お使いの LAN カードを選択します。**

7. [IP アドレス] タブ画面で「DHCP サーバーから IP アドレスを取得する」を選択します。





「DHCP サーバ機能」を使用しない→「Q & A Q15」(P.144)

8. [OK] ボタンをクリックして、[ネットワーク] ウィンドウに戻ります。

9. [閉じる] ボタンをクリックします。

パソコンを再起動するかを確認するメッセージが表示されます。

10. [はい] ボタンをクリックし、パソコンを再起動します。

設定した内容は、再起動後に有効になります。

2

パソコンの設定（Windows® 2000）

パソコンにTCP/IPがインストールされていることを確認します。
Windowsデスクトップの設定で「Webスタイル」を指定してある場合は、「ダブルクリック」と記載してあるところは「シングルクリック」で操作できます。

1. **［コントロールパネル］ウィンドウを開き、［ネットワークとダイヤルアップ接続］アイコンをダブルクリックします。**

2. **［ローカル接続］アイコンをダブルクリックします。**

［ローカルエリア接続状態］ダイアログボックスが表示されます。

3. **［プロパティ］ボタンをクリックします。**

［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。



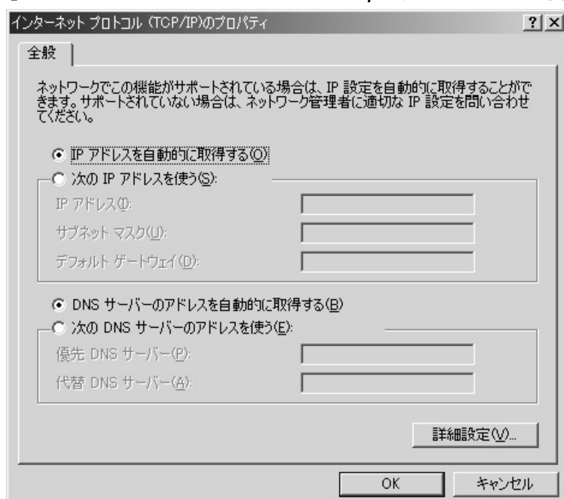
4. **一覧にインターネットプロトコル（TCP/IP）が含まれていることを確認します。**

補足 一覧にインターネットプロトコル（TCP/IP）が見つからない場合は、TCP/IPのインストールが必要です。Windows® 2000のマニュアルを参照して、インストールしてください。

5. **一覧から「インターネットプロトコル（TCP/IP)」をクリックして選択します。**

6. ［プロパティ］ボタンをクリックします。

［インターネットプロトコル（TCP/IP）のプロパティ］ダイアログボックスが表示されます。



7. パソコンの IP アドレスを設定します。

- NetVehicle の「DHCP サーバ機能」を利用する場合
  「IP アドレスを自動的に取得する」を選択します。
- NetVehicle の「DHCP サーバ機能」を利用しない場合
  「次の IP アドレスを使う」を選択し、IP アドレスを「192.168.1.2」、サブネットマスクを「255.255.255.0」、デフォルトゲートウェイを「192.168.1.1」に指定します。

8. DNS サーバの IP アドレスを設定します。

- DNS サーバの IP アドレスが固定の場合

「優先 DNS サーバ」、「代替 DNS サーバ」にそれぞれの DNS サーバの IP アドレスを指定してください。なお、各サーバの IP アドレスはネットワーク管理者にお問い合わせください。

- DNS サーバの IP アドレスが固定でない場合

「次の DNS サーバーのアドレスを自動的に取得する」を選択します。

9. ［OK］ボタンをクリックして、［ローカルエリア接続のプロパティ］ダイアログボックスに戻ります。

10. ［OK］ボタンをクリックします。

パソコンを再起動するかを確認するメッセージが表示されます。

11. ［はい］ボタンをクリックし、パソコンを再起動します。

設定した内容は、再起動後に有効になります。

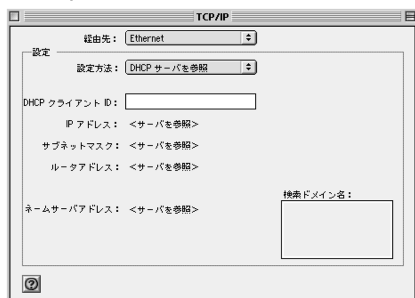
パソコンの設定（Mac OS 9）

Macintosh で TCP/IP を有効にする方法を説明します。

1. **アップルメニューから［コントロールパネル］を選択します。**

2. **サブメニューから［TCP/IP］を選択します。**

［TCP/IP］ウィンドウが開きます。



3. **「経由先」のプルダウンメニューから「Ethernet」を選択します。**

4. **「設定方法」で「DHCP サーバを参照」を選択します。**

必要に応じて、「検索ドメイン名」も入力します。

5. **［TCP/IP］ウィンドウを閉じます。**

6. **ダイアログで［保存］ボタンをクリックします。**

設定した内容が保存され、有効になります。

WWW ブラウザを用意する

NetVehicleを利用するには、Microsoft Internet Explorer 4.0以降または Netscape Navigator3.0以降（ただしNetscape 6を除く）が必要です。ブラウザの設定が、「Proxy（プロキシ）サーバ機能」を利用しないようになっていることを確認してください。

2

こんな事に気をつけて

すでにWindows® 95/98の「ダイヤルアップネットワーク」でモデムやTAをお使いの場合は、ブラウザ起動時の設定を次のように変更してください。

1. ［コントロールパネル］-［インターネットオプション］-［インターネットのプロパティ］-［接続］タブの順に選択して、「接続タブ」を表示する。
2. ダイヤルアップの設定で「ダイヤルしない」を選択する。
3. ［OK］ボタンをクリックする。

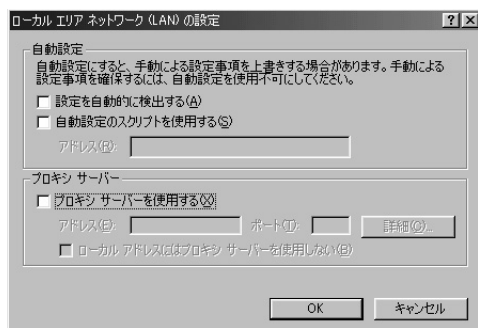
Microsoft Internet Explorer 5.5

Microsoft Internet Explorer 5.5 の場合は、次のように確認します。

1. ［ツール］メニューから「インターネットオプション」を選択します。

2. インターネットオプション画面の「接続」タブで、LANの設定の［LANの設定］ボタンをクリックします。

3. 「プロキシサーバーを使用する」が選択されていないことを確認します。



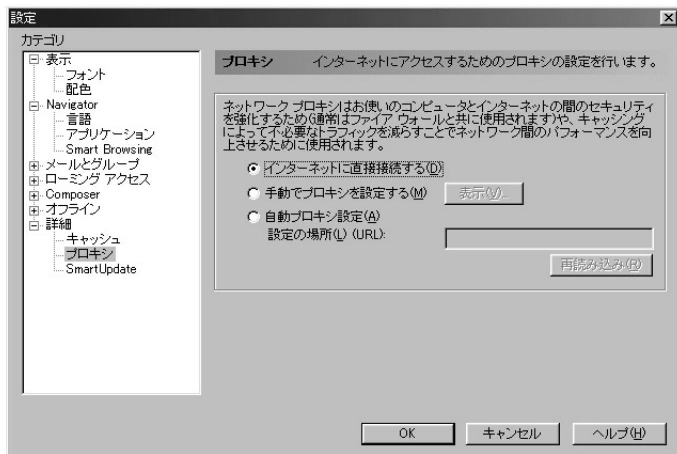
Netscape Communicator 4.7

Netscape Communicator 4.7 の場合は、次のように確認します。

1. ［編集］メニューから「設定」を選択します。

2. 設定画面の「カテゴリ」で「詳細－プロキシ」を選択します。

3. 「インターネットに直接接続する」が選択されていることを確認します。



補足 Proxy サーバを使用する場合は、下記を参考にして NetVehicle だけを Proxy の対象外にしてください。

Microsoft Internet Explorer 5.5 の場合は、次のように設定します。

1.［ツール］メニューから「インターネットオプション」を選択します。

2. インターネットオプション画面の「接続」タブで、LAN の設定の［LAN の設定］ボタンをクリックします。

3. プロキシサーバーの「プロキシサーバーを使用する」が選択されていることを確認し、[詳細] ボタンをクリックします。

4.「HTTP」にプロバイダの Proxy サーバを指定します。

5. 例外の「次で始まるアドレスにはプロキシを使用しない」に NetVehicle の IP アドレス（192.168.1.1）を指定します。

Netscape Communicator 4.7 の場合は、次のように設定します。

1.［編集］メニューから「設定」を選択します。

2. 設定画面の「カテゴリ」で「詳細－プロキシ」を選択します。

3.「手動でプロキシを設定する」を選択し、［表示］ボタンをクリックします。

4.「HTTP」にプロバイダの Proxy サーバを指定します。

5. 例外の「次ではじまるドメインにはプロキシサーバを使用しない」にNetVehicleのIPアドレス（192.168.1.1）を指定します。



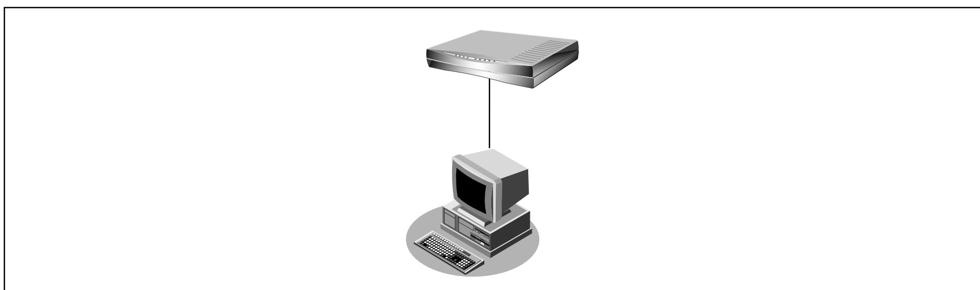
NetVehicleとパソコンをつなぐ

⚠警告

NetVehicle および接続する機器の電源を切ってから、つないでください。

パソコンとつなぐ

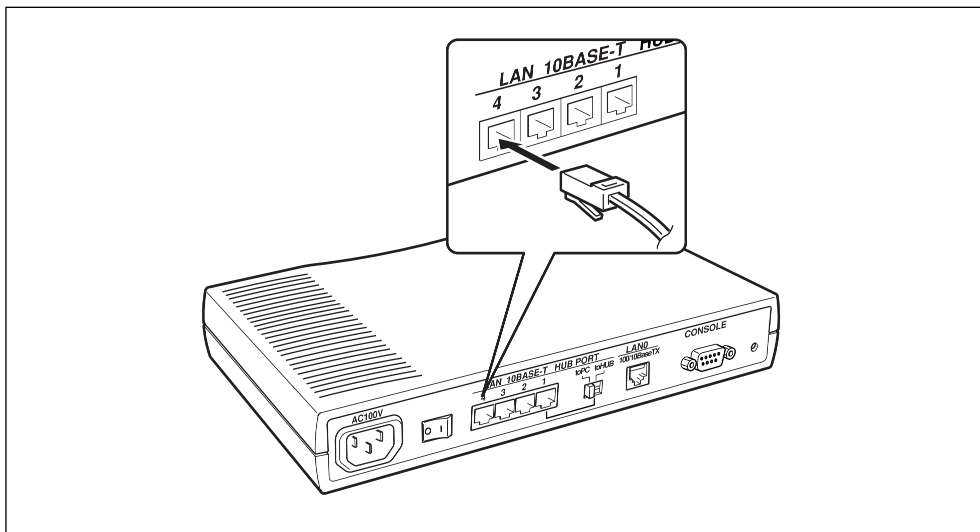
プライベート LAN 以外の形態のネットワークを構築する前には、NetVehicle の設定が必要です。設定を行うときは NetVehicle とパソコンを 1 対 1 でつないでください。すでにネットワークを構築している場合も、1 台のパソコンを一時的にネットワークから切り離し、NetVehicle につないでから設定します。



1. **パソコンと NetVehicle の電源を切ります。**

2. **パソコンの 10BASE-T ポートに 10BASE-T ケーブルの一方の端を差し込みます。**

3. **NetVehicleのLAN1側の10BASE-Tポートに10BASE-Tケーブルのもう一方の端を差し込みます。**



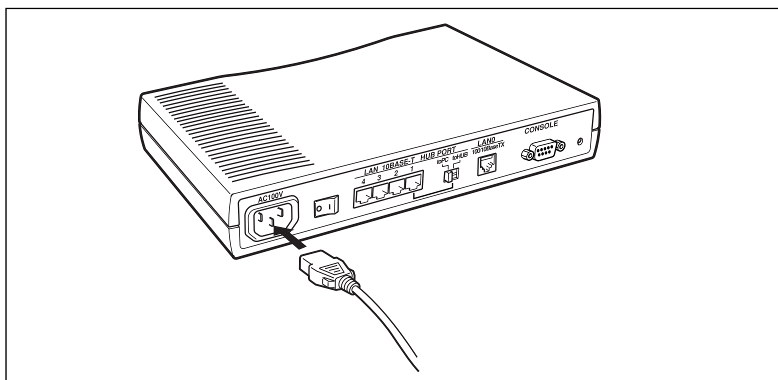
こんな事に気をつけて

- ご購入時は、LAN1 側の 10BASE-T ポートからのみ設定できます。
- 本製品の 10BASE-T（HUB）ポートに 10/100BASE-TX 機器（PC、ワークステーション、HUB など）を接続してお使いになる場合は、接続機器のポートを“ 10Mbps/ 半二重（Half-Duplex）”にしてお使いになることをお勧めします。
- 速度（10M/100M）および全二重/半二重（Full-Duplex/Half-Duplex）自動検出モードにてお使いになると、正しく接続できないことがあります。万が一、速度自動検出モードにて正しく接続できない場合は、一度 LAN ケーブルを抜き、機器の設定を“ 10Mbps/ 半二重（Half-Duplex）”に変更後、再接続を行ってください。

NetVehicle を電源につなぐ

電源ケーブルの先は、2 ピンになっています。通常の電源コンセント（2 穴式）にそのまま差し込みます。電源ケーブルに付いているアース線の先をコンセントの FG ネジに取り付けます。

1. 本体背面に電源ケーブルを差し込みます。

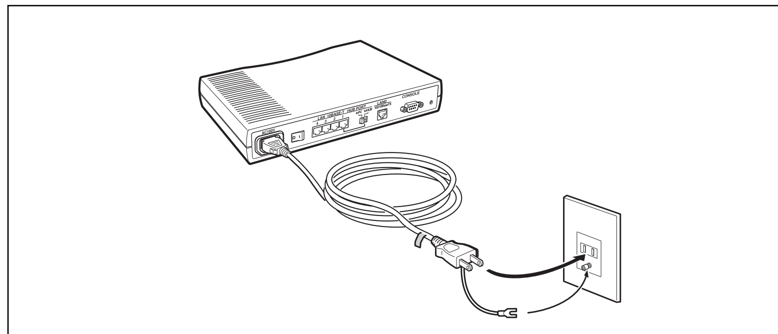


2. アース線の先についている FG 端子をコンセントの FG ネジに取り付けます。

⚠警告

感電のおそれがあります。アース線は必ず接続してください。

3. 電源ケーブルを、電源コンセントに差し込みます。



⚠警告

NetVehicle の電源スイッチが「○」側へ押されていることを確認してから、電源コンセントに差し込んでください。



NetVehicle を設定する

NetVehicle とパソコンの電源を入れる

1. **NetVehicle の電源を入れます。**

2. **NetVehicle が起動したことを確認します。**

補足 電源が入ると、NetVehicle は自動的に装置の状態を診断します。 このとき、POWER ランプ以外が点滅します。次に CHECK,LAN0,100M,FULL,LAN1 ランプが同時に緑色で約 2 秒間点灯します。装置に異常がない場合は、CHECK ランプが消灯して、 起動が完了します。

3. **パソコンの電源を入れます。**

4. **IP 通信の状態を確認します。**

補足 Windows® 95/98/Me には、IP アドレスやアダプタアドレス（MAC アドレス）など現在の IP 設定情報を確認できるコマンドがあります。以下のように操作します。
1.［スタート］-［ファイル名を指定して実行］を選択する。
2.「winipcfg.exe」を指定する。

WindowsNT®/Windows® 2000 の場合には、「ipconfig.exe」で確認できます。

WWWブラウザを起動してNetVehicleのトップページを表示させる

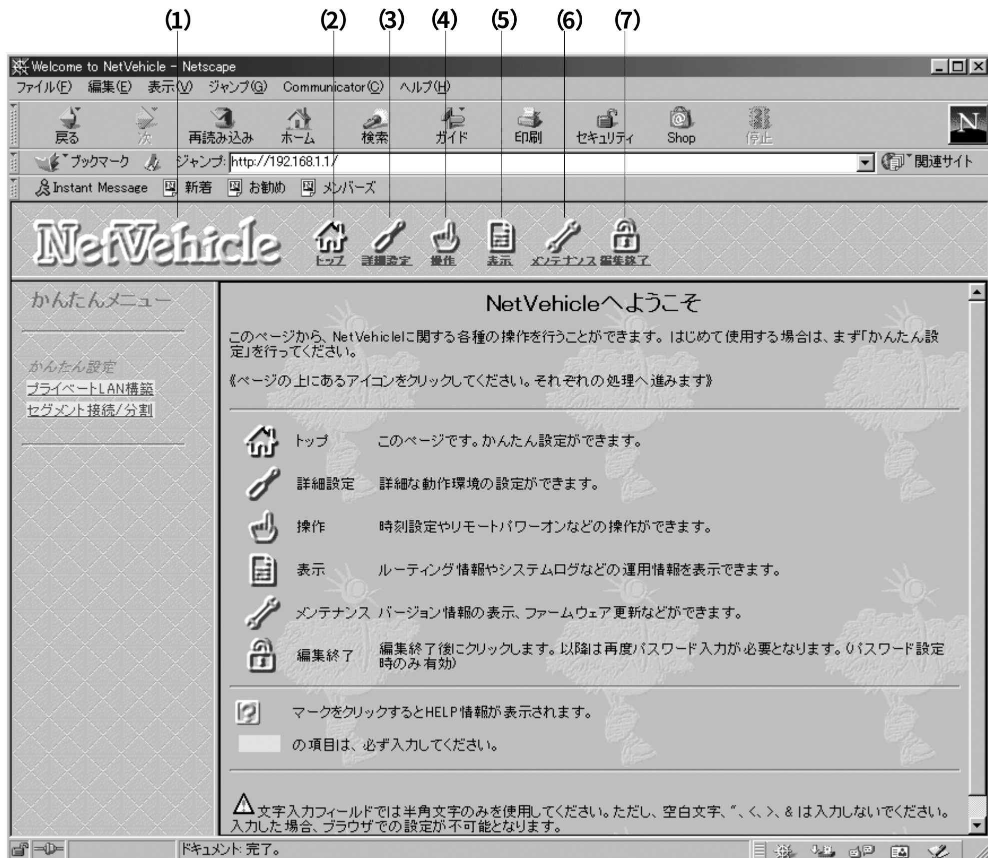
参照 **WWW ブラウザの設定→「WWW ブラウザを用意する」（P.31）**

1. **WWW ブラウザを起動します。**

2. NetVehicle の URL「http://192.168.1.1/」を指定します。

NetVehicle のトップページが表示されます。

補足 ProxyDNS をご利用の場合は「http://nvmenu/」でも表示されます。



画面上部のフレームに表示されるアイコンをクリックすると、ブラウザの表示が変わります。

(1) NetVehicle ロゴ	クリックすると、トップメニューが表示されます。
(2)［トップ］アイコン	クリックすると、かんたんメニューが表示されます。 かんたんメニューには「かんたん設定」があります。 「かんたん設定」では、ネットワークに接続するための基本設定が行えます。
(3)［詳細設定］アイコン	クリックすると、詳細設定メニューが表示されます。 「詳細設定」では、「かんたん設定」より詳細な情報を設定できます。
(4)［操作］アイコン	クリックすると、操作メニューが表示されます。
(5)［表示］アイコン	クリックすると、表示メニューが表示されます。
(6)［メンテナンス］アイコン	クリックすると、メンテナンスメニューが表示されます。
(7)［編集終了］アイコン	クリックすると、すぐに設定操作を終了できます（ログインパスワードが設定されている場合のみ有効）。

設定方法を選ぶ

設定方法には「かんたん設定」と「詳細設定」の2つがあります。
通常のご利用では、「かんたん設定」で十分です。「かんたん設定」で設定したあとで、必要な設定に関しては、「詳細設定」で設定を追加する方法をお勧めします。
なお、プライベートLANを構築する場合は、NetVehicleを既存のLANに接続するだけで使用できます。

2

ご購入時の状態で使用する場合

ご購入時の状態のNetVehicleは、すぐにプライベートLANが使える設定になっています。既存のLANにDHCPサーバがある場合はパソコンを接続するだけで使用できます。通信条件を変更したい場合は、「かんたん設定」で設定します。


プライベートLAN接続→「「かんたん設定」で設定する（プライベートLAN接続）」（P.50）

「かんたん設定」で設定する場合

「かんたん設定」には、「プライベートLAN構築」と「セグメント接続／分割」の2つがあります。

（1）プライベートLAN接続
新規にLANを構築し、既存のネットワーク上にあるIPアドレスを1つだけ使って、複数のパソコンから通信する場合の設定です。CATVインターネット接続や既存のネットワークに一時的にLANをつなぎたいときに使います。


プライベートLAN接続→「「かんたん設定」で設定する（プライベートLAN接続）」（P.50）

（2）セグメント接続／分割
既存のネットワークどうしを接続したり、分割したりする場合の設定です。
ネットワークに接続できるパソコン台数を超えたり、通信トラフィックが増加した場合など、ネットワークを分割したいときに使います。


セグメント接続／分割→「「かんたん設定」で設定する（セグメント接続／分割）」（P.54）

「かんたん設定」で設定する場合は、設定終了時に［設定終了］ボタンをクリックする必要があります。［設定終了］ボタンをクリックすると、NetVehicleが再起動され、データ通信中の場合、データは切断されます。

「詳細設定」で設定する場合

NetVehicleの持つ便利な機能を使いこなしたいときに使う設定です。
通信を制御したり、DHCP機能やDNS機能などをお使いになる場合に使用します。
「詳細設定」では、複数のページで設定が必要な場合、それぞれのページで設定した情報を［更新］ボタンをクリックして更新し、最後に［設定反映］ボタンをクリックすると設定が有効になります。データ通信中の場合、データは切断されます。


詳細設定→「「詳細設定」で設定する」（P.57）


こんな事に気をつけて

「詳細設定」で設定したあとに「かんたん設定」で設定すると、「詳細設定」で設定した内容が無効になるので注意してください。
ただし、パスワード情報、ファームウェア更新情報は有効です。



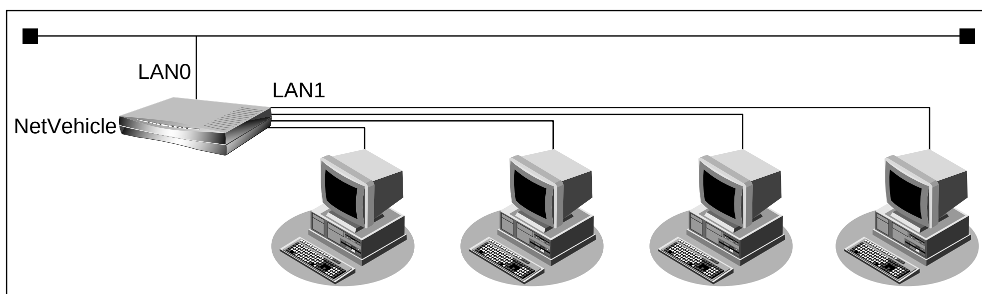
NetVehicleとパソコンをLANにつなぐ

NetVehicleの設定が終了したら、パソコン側の設定を有効にするためブラウザとパソコンのシステムを終了し、すべての電源を切ります。
ここでは、NetVehicle とパソコンを 10BASE-T ケーブルでつなぎ、LAN を構築する方法を説明します。

LAN を構築する

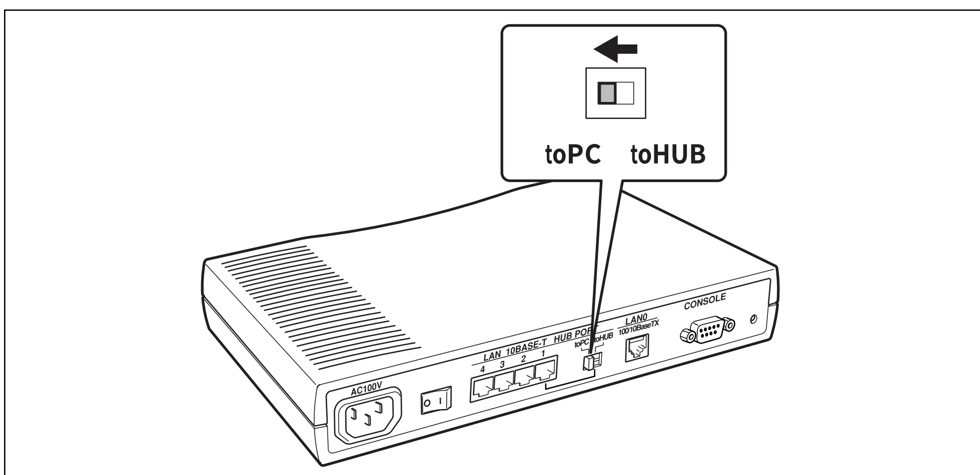
利用するパソコンが 4 台以下の場合は、LAN1 側の空いているポートに 10BASE-T ケーブルの端を差し込んでパソコンとつなぎます。
利用するパソコンが 5 台以上の場合は、LAN1 側の HUB ポート 1 とハブ装置をカスケード接続します。

利用するパソコンが 4 台以下の場合



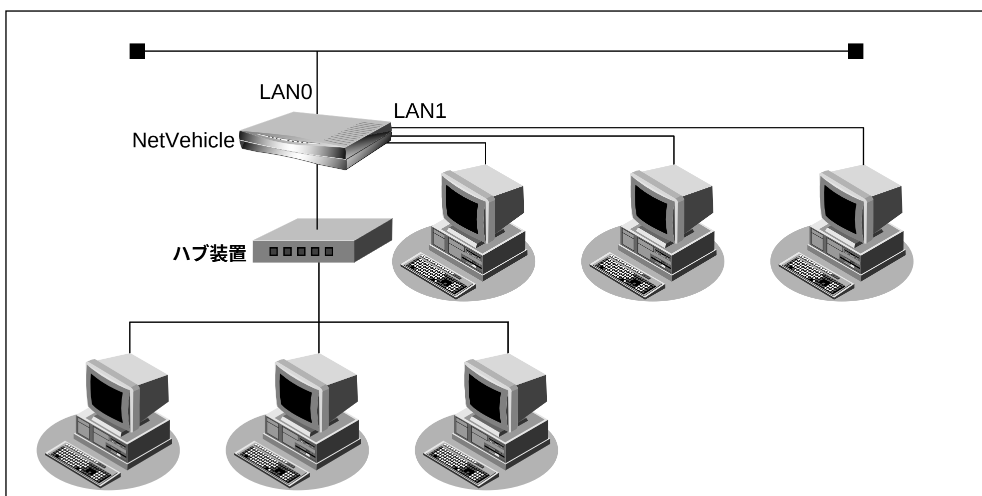
1. **10BASE-T ケーブルで NetVehicle の LAN0 側のポートと既存の LAN 側を接続します。**

2. **NetVehicle の背面にある HUB ポート 1 切り替えスイッチが「toPC」側にあることを確認します。**



3. **10BASE-T ケーブルで NetVehicle の LAN1 側の空いているポートとパソコンをつなぎます。**

利用するパソコンが 5 台以上の場合



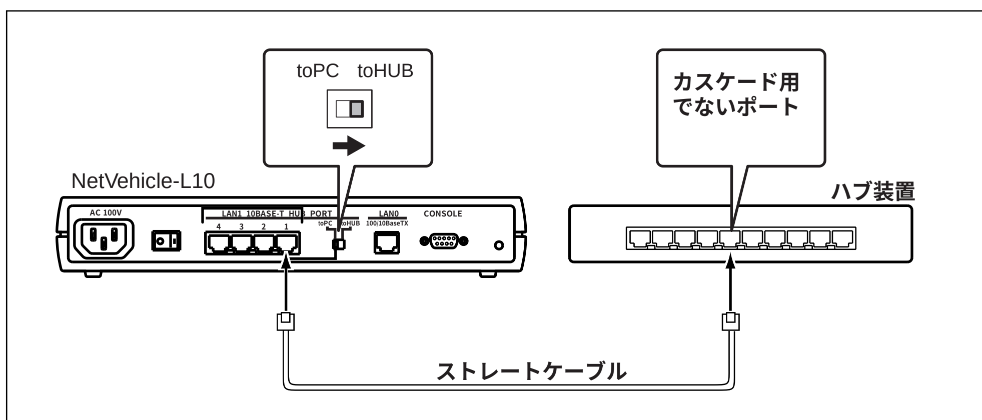
1. **10BASE-T ケーブルで NetVehicle の LAN0 側のポートと既存の LAN 側を接続します。**

2. **NetVehicle の背面にある HUB ポート 1 切り替えスイッチが「toHUB」側にあることを確認します。**

3. **10BASE-T ケーブル（ストレート）で HUB ポート 1 とハブ装置のポートをつなぎます。**

 **こんな事に気をつけて**

外づけハブ装置のカスケード用ポートとは接続しないでください。



4. **パソコンとハブ装置を 10BASE-T ケーブルでつなぎます。**

NetVehicle とパソコンの電源を入れる

1. **NetVehicle の電源を入れます。**

2. **NetVehicle が起動したことを確認します。**

補足 電源が入ると、NetVehicle は自動的に装置の状態を診断します。 このとき、POWER ランプ以外が点滅します。次に CHECK,LAN0,100M,FULL,LAN1 ランプが同時に緑色で約２秒間点灯します。装置に異常がない場合は、CHECK ランプが消灯して、 起動が完了します。

3. **パソコンの電源を入れます。**

こんな事に気をつけて

設定した内容を有効にするために、NetVehicle の電源を入れてから、パソコンの電源を入れてください。



設定内容を確認 / 変更する

NetVehicle は LAN につないだままの状態で設定内容を確認 / 変更できます。NetVehicle の IP アドレスを変更した場合は、ブラウザ上で新しい NetVehicle の IP アドレスを URL に指定してください。


こんな事に気をつけて

NetVehicle の IP アドレスを変更した場合は、パソコン側の設定も合わせて変更してください。

「かんたん設定」で設定した場合の確認 / 変更

「かんたん設定」で設定した内容の確認 / 変更は、「かんたん設定」で行うと便利です。操作方法は設定を行う場合と同じです。
設定ページには、前回設定した内容が表示されます。
「かんたん設定」で設定する場合は、設定終了時に［設定終了］ボタンをクリックしないと、変更した内容は有効になりません。［設定終了］ボタンをクリックすると、NetVehicle が再起動され、データ通信中の場合、データ通信は切断されます。


こんな事に気をつけて

「詳細設定」で設定したあとに「かんたん設定」で設定すると、「詳細設定」で設定した内容が無効になるので注意してください。
ただし、パスワード情報、ファームウェア更新情報は有効です。

「詳細設定」で設定した場合の確認 / 変更

「詳細設定」で設定した内容を確認 / 変更する場合の操作方法は設定を行う場合と同じです。
設定ページには、前回設定した内容が表示されます。
［設定反映］ボタンをクリックしないと、変更した内容は有効になりません。［設定反映］ボタンをクリックすると、NetVehicle が再起動され、データ通信中の場合、データ通信は切断されます。



◆ NetVehicle を使いこなすために

「第 5 章　NetVehicle の便利な機能を活用する」または NetVehicle サポートページ（http://telecom.fujitsu.com/jp/products/nv）では、さらに詳しい情報を紹介しています。



NetVehicleでCATVインターネット接続する

この章では、
CATVインターネット接続の基本的な接続および設定方法を説明しています。



CATV インターネット接続とは

CATV インターネット接続とは、CATV 事業者が提供するインターネット接続サービスです。CATV インターネット接続には、ケーブルモデム接続とダイヤルアップ接続の 2 つの接続形態があります。ケーブルモデム接続は、ケーブルテレビ網を利用したもので、CATV事業者が提供するケーブルモデムに接続する形態です。ダイヤルアップ接続とは、CATV電話サービスを利用したもので、パソコンにモデムを接続する形態です。NetVehicle を使用して CATV インターネット接続する場合は、「ケーブルモデム接続」の形態となり、CATV 事業者との契約が必要です。接続にあたっては、CATV 事業者の指示に従ってください。



◆ケーブルモデム

ケーブルテレビ網に接続するための専用モデムで、CATV インターネット接続サービスに必要な機器です。パソコン（LAN ボード）とは 10BASE-T ケーブルで接続します。通常、CATV サービス加入時に CATV 事業者より貸し出され、宅内工事の際に設置されます。

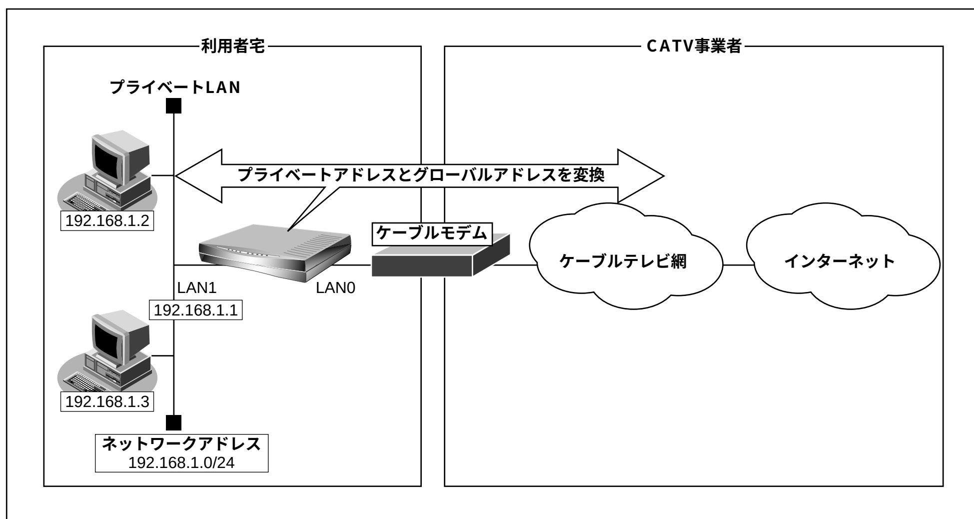


CATVインターネット接続の設定を行う

NetVehicleを使ったCATVインターネット接続は、CATV事業者が提供するインターネット接続サービスをプライベートLAN上の複数のパソコンから利用するための接続形態です。NetVehicleとCATV事業者が提供するケーブルモデムを接続することで、プライベートLAN上のパソコンからインターネット接続サービスを利用できます。
NetVehicleのアドレス変換機能がCATV事業者側のネットワークと利用者側のプライベートLANとの間で動作し、プライベートLAN側のIPアドレスを外部から隠すため、セキュリティが確保できます。
CATVインターネット接続は「かんたん設定（プライベートLAN構築）」で設定します。CATV事業者側（LAN0側）の設定方法はCATV事業者の指示に従ってください。なお、IPアドレスやDHCP機能の変更が必要な場合は、詳細設定で設定することができます。

3

補足 利用者は、プライベートLAN側の情報のみ設定できます。



通信条件

[CATV事業者側（LAN0）]

- CATV事業者の指示に従ってください。

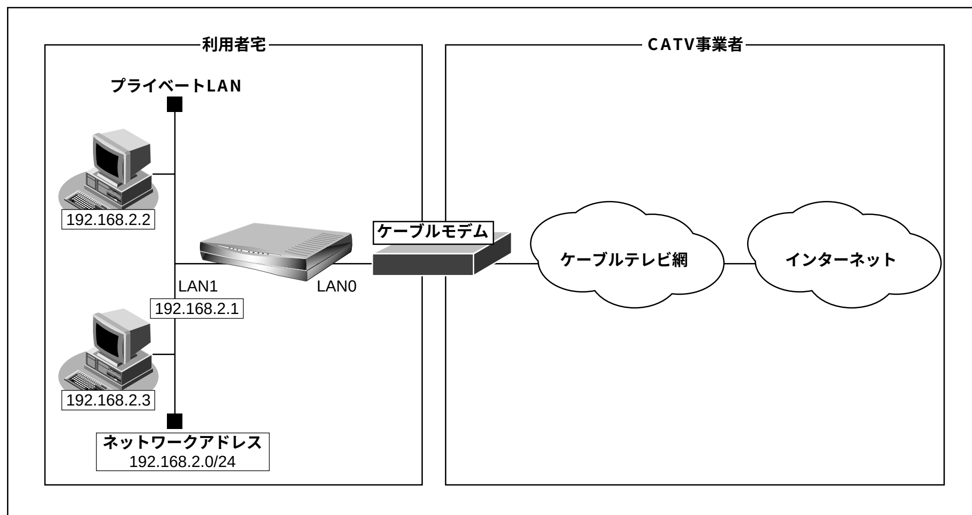
[プライベートLAN側 （LAN1）]

- NetVehicleのIPアドレス　　：192.168.1.1
- ネットワークアドレス / ネットマスク　　：192.168.1.0/24
- DHCPサーバ機能を使用する

こんな事に気をつけて

契約したCATV事業者によって設定方法が異なります。実際の設定は、CATV事業者の指示に従ってください。
本書では、プライベート LAN 側の設定を詳細設定で行う場合の例を記述します。

以下に、プライベート LAN 側の通信条件が下記の場合に詳細設定で設定する手順を示します。



通信条件

［CATV 事業者側 （LAN0）］

- CATV 事業者の指示に従ってください。

［プライベート LAN 側 （LAN1）］

- NetVehicle の IP アドレス ：192.168.2.1
- ネットワークアドレス / ネットマスク ：192.168.2.0/24
- DHCP サーバ機能を使用する

こんな事に気をつけて

文字入力フィールドには半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「 ”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

詳細設定で設定する

1. **NetVehicle のトップページで詳細設定のアイコンをクリックします。**

「詳細設定」ページが表示されます。

3

詳細設定で LAN1 情報を設定する

2. **詳細設定メニューで「LAN1 情報」をクリックします。**

「LAN1 情報設定」ページが表示されます。

3. **［IP アドレス］で以下の項目を設定します。**

- IP アドレス →指定する
- IP アドレス → 192.168.2.1
- ネットマスク → 24
- ブロードキャストアドレス →ネットワークアドレス＋オール 1

［IPアドレス］
IPアドレス
DHCPで自動的に取得する
指定する
IPアドレス 192 . 168 . 2 . 1
ネットマスク 24 (255.255.255.0)
ブロードキャストアドレス ネットワークアドレス＋オール1

4. **［DHCP 機能］で［修正］ボタンをクリックします。**

「DHCP 情報設定」ページが表示されます。

5. **［DHCP 機能］で以下の項目を設定します。**

- LAN1 →サーバ機能を使用する

LAN1
使用しない
リレー機能を使用する
DHCPサーバIPアドレス
サーバ機能を使用する
割当て先頭IPアドレス 192 . 168 . 2 . 2
割当てアドレス数 32
リース期間 1 日
ネットマスク広報 24 (255.255.255.0)

6. **［更新］ボタンをクリックします。**

「LAN1 情報設定」ページに戻ります。

7. **［更新］ボタンをクリックします。**

8. **［設定反映］ボタンをクリックします。**

設定した内容が有効になります。



NetVehicle で ネットワーク間接続する

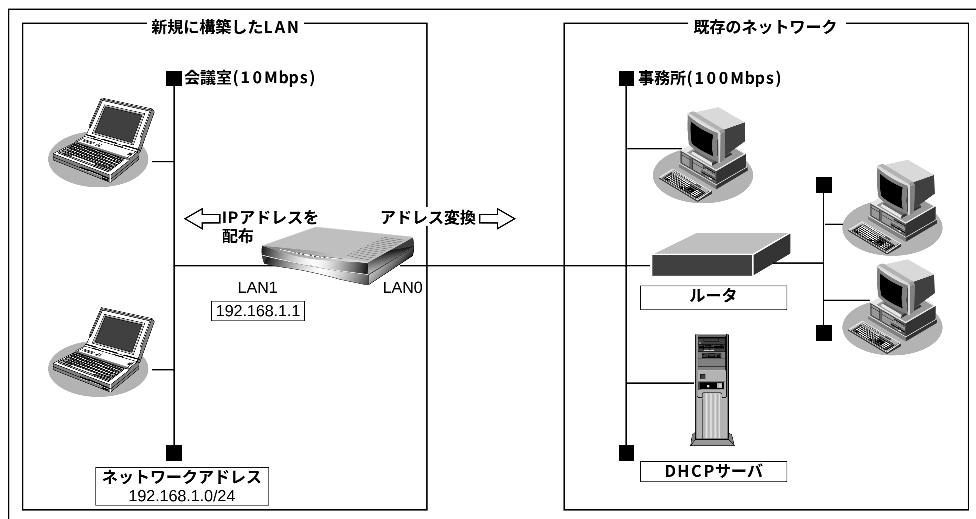
この章では、
ネットワーク間接続するための手順や設定方法について説明します。



「かんたん設定」で設定する（プライベート LAN 構築）

「かんたん設定」では、ネットワークを接続するための基本的な設定を 1 つのページで行うことができます。プライベート LAN 側では、マルチ NAT 機能を利用しているので、割り当てられた 1 つのグローバルアドレスを使って、複数台のパソコンからネットワークにアクセスできます。また、DHCP サーバ機能が動作しているため、パソコンの IP アドレスの管理が必要ないため簡単に LAN を構築できます。「かんたん設定」で設定したあとに、必要な情報を「詳細設定」で追加、および変更することもできます。ここでは、以下の条件で一時的に会議室に LAN を構築し、事務所のネットワークと接続する場合を例に説明します。

NetVehicle の IP アドレスを変更しない場合



通信条件

［事務所側］

- 転送レートは 100Mbps
- IP アドレスは自動的に取得する

［会議室側］

- 転送レートは 10Mbps
- NetVehicle の IP アドレス　：192.168.1.1
- ネットワークアドレス / ネットマスク　：192.168.1.0/24

［その他の条件］

- 管理者パスワードを設定する
  新しいログインパスワード　：himitu

この例の場合、ご購入時の状態の NetVehicle では、NetVehicle の電源を入れるだけで通信が行えます。ただし、管理者パスワードだけは詳細設定で設定する必要があります。

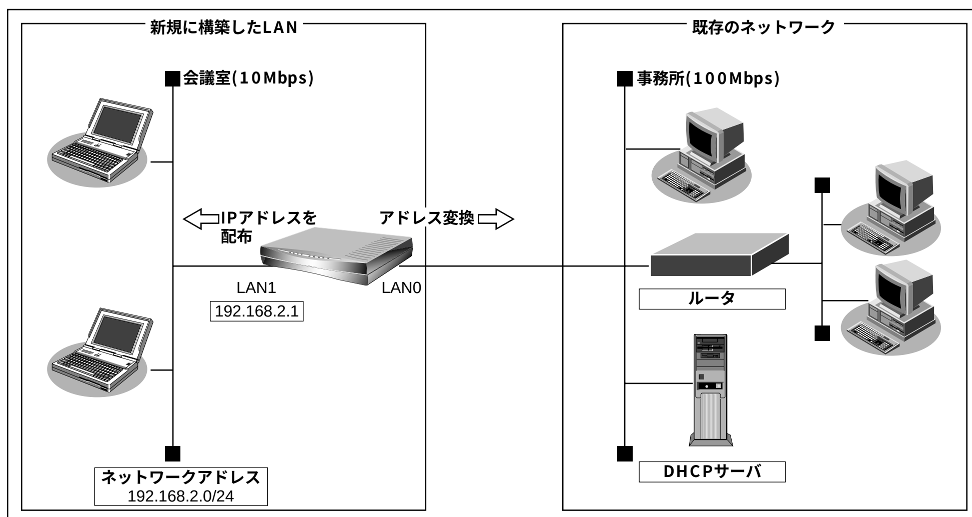

管理者パスワードを設定する→「詳細設定」で設定する（P.61）

こんな事に気をつけて

- セキュリティ確保のため管理者パスワードを設定することを強く推奨します。設定しない場合、ネットワーク上の誰からでもアクセスできるため非常に危険です。
- 「プライベート LAN 構築」の「かんたん設定」では、LAN1 側で自動的に DHCP サーバが動作します。DHCP サーバが広報する情報（デフォルトルータ、DNS サーバ、ドメイン名）には LAN1 側のネットワーク構成に応じた情報を設定してください。

NetVehicle の IP アドレスを変更する場合

「プライベート LAN 構築」では、プライベート LAN 側（LAN1 側）のネットワークアドレスを変更することができます。
以下に、プライベート LAN 側（LAN1 側）のネットワークアドレスを 192.168.2.0/24 に変更する手順を示します。



こんな事に気をつけて

文字入力フィールドには半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「 ”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

1. かんたんメニューで「プライベート LAN 構築」をクリックします。

「プライベート LAN 構築かんたん設定」ページが表示されます。

補足 かんたんメニューは、ブラウザ画面上部の[トップ]アイコンをクリックして表示させることができます。

この例では、LAN0 側は DHCP サーバから自動的に情報を取得するので、LAN1 側のみを設定します。

2. ［LAN1］で以下の項目を指定します。

- IP アドレス　→ 192.168.2.1
- ネットマスク　→ 24
- デフォルトルータ広報　→ 192.168.2.1
- DNS サーバ広報　→ 192.168.2.1

［LAN1］

IPアドレス		192 . 168 . 2 . 1
ネットマスク		24 (255.255.255.0)
DHCPサーバ	デフォルトルータ広報	192 . 168 . 2 . 1
	DNSサーバ広報	192 . 168 . 2 . 1
	ドメイン名広報	

3. 設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に通信できる状態になります。

こんな事に気をつけて

- NetVehicle の LAN1 側の IP アドレスを変更した場合、以下に示す 2 つの操作が必要です。
  - ・LAN1 側に接続しているパソコンの IP アドレスも変わるので、再度、DHCP サーバから割り当ててもらう必要があります。
  - ・再起動後に NetVehicle にアクセスするためには、URL で指定する IP アドレスに変更後の IP アドレスを指定する必要があります。
- LAN1 側に接続するネットワーク上のパソコンは、IP アドレスを自動的に取得する設定にしてください。IP アドレスを固定的に設定していると、NetVehicleが配布するIPアドレスと重なり、矛盾が生じる場合があります、なお、常時同じ IP アドレスを取得したい場合は、詳細設定の「ホストデータベース情報」に IP アドレスと MAC アドレスを設定してください。

補足　設定した内容を巻末の設定メモに転記しておくと、あとで確認が必要になったときに便利です。



◆ NAT（マルチ NAT）

グローバルアドレスとプライベートアドレスの変換を行うアドレス変換機能のことです。

NetVehicle は以下の 2 つの変換方法をサポートしています。
・グローバルアドレスとプライベートアドレスを 1 対 1 に対応付ける基本 NAT
・IP アドレスとポート番号を組み合わせて一つのグローバルアドレスに複数のプライベートアドレスを対応付けるマルチ NAT



NAT（マルチ NAT）→「マルチ NAT 機能（アドレス変換機能）を使う」（P.64）



◆ DHCP サーバ機能

DHCPサーバ機能は、ネットワークに接続されているパソコンに対してIPアドレスなどの情報を自動的に割り当てる機能です。



DHCP サーバ機能→「DHCP サーバ機能 」（P.83）



◆転送レート

NetVehicleのインタフェースの動作モード（通信速度と通信方式）のことです。NetVehicleのLAN0インタフェースの通信速度は10Mbpsと100Mbpsが選択できます。100Mbpsでは通信方式として半二重と全二重のいずれかが選択できます。自動認識の設定をすることで、自動的に通信速度と通信方法を認識させることもできます。自動認識でハブ装置とうまく接続できない時は、手動でも設定できます。

◆半二重／全二重

通信方式には、半二重通信と全二重通信があります。共に双方向通信できますが、半二重通信は同時には双方向通信できません。

省略値について

かんたん設定（プライベートLAN構築）時に適用される主な省略値を示します。

○：変更可能　　×：変更不可能

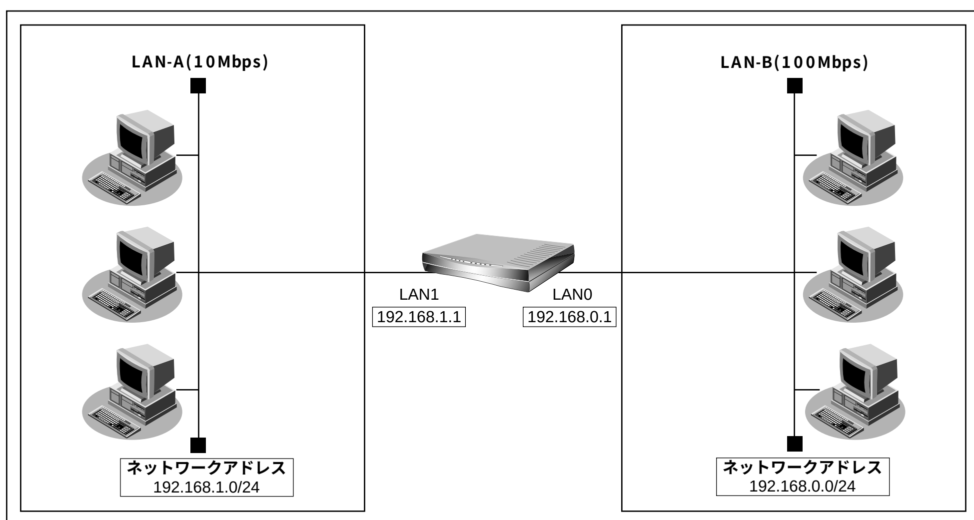
	項　　目	適用される省略値	かんたん設定での設定変更
LAN0	IPアドレス	DHCPクライアント機能により自動的に取得する	○
	ネットマスク	DHCPクライアント機能により自動的に取得する	○
	セカンダリIPアドレス	なし	×
	デフォルトルータ	DHCPクライアント機能により自動的に取得する	○
	DNSサーバアドレス	DHCPクライアント機能により自動的に取得する	○
	DHCPサーバ機能	使用しない	×
	NAT機能	マルチNATを使用する ・グローバルアドレス：LAN0側のIPアドレス ・アドレス個数：1個 ・アドレス割当タイマ：5分	×
	ダイナミックルーティング ・RIP送信 ・RIP受信	（グローバルIPアドレス1個） ルーティングプロトコルを使用しない RIP-V1を使用する	×
	転送レート	自動認識	○
LAN1	IPアドレス	192.168.1.1	○
	ネットマスク	24（255.255.255.0）	○
	セカンダリIPアドレス	なし	×
	DHCPサーバ機能 ・割り当て先頭IPアドレス ・割り当てアドレス数	使用する NetVehicleのLAN側のIPアドレス、 ネットマスクから求めたネットワークアドレス＋2 253	×
	デフォルトルータ広報	192.168.1.1	○
	DNSサーバ広報	192.168.1.1	○
	ドメイン名広報	なし	○
	NAT機能	使用しない	×
	ダイナミックルーティング ・RIP送信 ・RIP受信	 RIP-V1を使用する RIP-V1を使用する	×



「かんたん設定」で設定する（セグメント接続／分割）

ネットワークへの接続台数が増加したり、同一ネットワーク上に大量データを送受信するホストがあると、トラフィックが増加し、通信性能が劣化する場合があります。このような場合、ネットワークを分割することで、トラフィックを分散することができます。NetVehicleは、2つのネットワークインタフェースを持っているので、簡単にネットワークを接続したり分割したりすることができます。「かんたん設定」では、接続や分割のための基本的な設定を 1 つのページ上で行うことができます。「かんたん設定」で設定したあとに、必要な情報を「詳細設定」で追加、および変更することもできます。ここでは、以下の条件で LAN-A と LAN-B をネットワーク間接続する場合を例に説明します。

NetVehicle の IP アドレスを変更しない場合



通信条件

[LAN-A 側]
- 転送レートは 10Mbps
- IP アドレス　：192.168.1.1
- ネットワークアドレス / ネットマスク　：192.168.1.0/24

[LAN-B 側]
- 転送レートは 100Mbps
- IP アドレス　：192.168.0.1
- ネットワークアドレス / ネットマスク　：192.168.0.0/24

[その他の条件]
- 管理者パスワードを設定する
- 新しいログインパスワード　：himitu

この例の場合、ご購入時の状態の NetVehicle では、かんたんメニューで「セグメント接続／分割」をクリックしたあと、「セグメント接続／分割かんたん設定」画面で「設定終了」をクリックするだけで通信が行えます。ただし、管理者パスワードだけは、詳細設定で設定する必要があります。



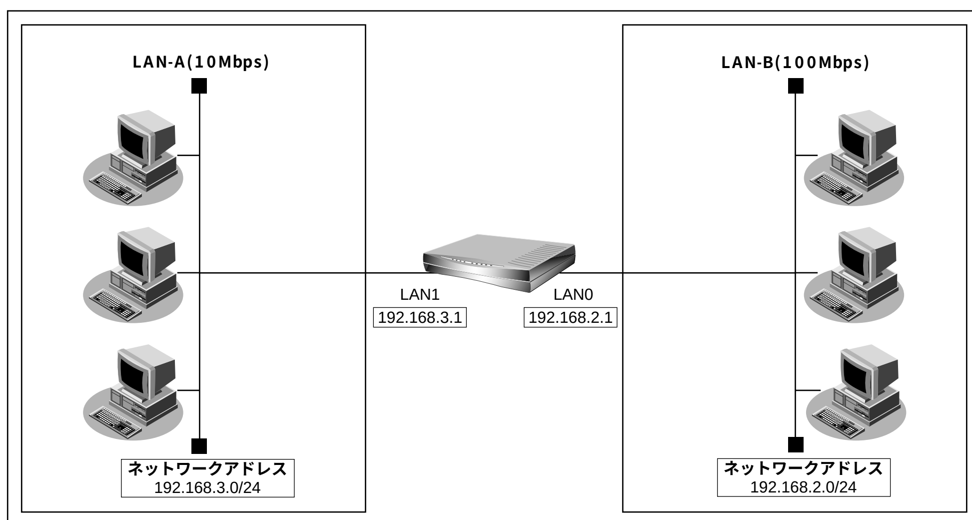
管理者パスワードを設定する→「「詳細設定」で設定する」(P.61)

こんな事に気をつけて

管理者パスワードを設定することを強く推奨します。設定しない場合、ネットワーク上の誰からでもアクセスできるため非常に危険です。

NetVehicle の IP アドレスを変更する場合

既存のネットワークどうしを接続/分割する場合には、それぞれのネットワーク環境に合わせた設定が必要です。「セグメント接続 / 分割」では、それぞれのネットワークのアドレスを設定できます。
以下に、LAN0 側のネットワークアドレスが 192.168.2.0/24、LAN1 側が 192.168.3.0/24 のネットワークを接続する手順を示します。



こんな事に気をつけて

文字入力フィールドには半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「 ”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

1. **かんたんメニューで「セグメント接続／分割」をクリックします。**
「セグメント接続／分割かんたん設定」ページが表示されます。

補足 かんたんメニューは、ブラウザ画面上部の［トップ］アイコンをクリックして表示させることができます。

2. 以下の項目を指定します。

[LAN0]

- IP アドレス　→ 192.168.2.1
- ネットマスク　→ 24

[LAN1]

- IP アドレス　→ 192.168.3.1
- ネットマスク　→ 24

[LAN0]

IPアドレス 192 . 168 . 2 . 1

ネットマスク 24 (255.255.255.0)

転送レート 自動認識

[LAN1]

IPアドレス 192 . 168 . 3 . 1

ネットマスク 24 (255.255.255.0)

3. 設定が終了したら、[設定終了] ボタンをクリックします。

再起動後に、通信できる状態になります。

こんな事に気をつけて

- NetVehicle の LAN1 側の IP アドレスを変更した場合、以下に示す 2 つの操作が必要です。
  - ・LAN1 側に接続しているパソコンの IP アドレスも合わせて変更する必要があります。
  - ・再起動後に NetVehicle にアクセスするためには、URL で指定する IP アドレスに変更後の IP アドレスを指定する必要があります。

補足 設定した内容を巻末の設定メモに転記しておくと、あとで確認が必要になったときに便利です。

省略値について

かんたん設定（セグメント接続／分割）時に適用される主な省略値を示します。

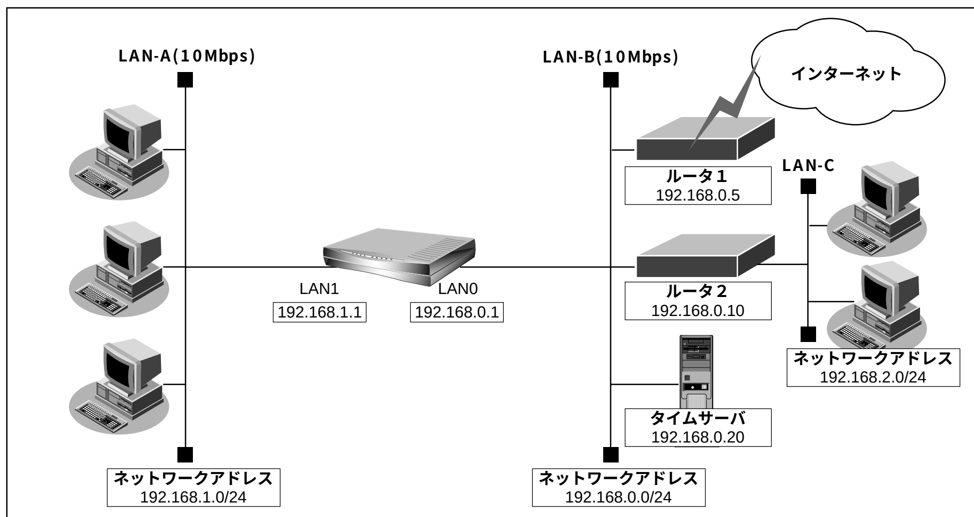
○：変更可能　　×：変更不可能

	項　　目	適用される省略値	かんたん設定での設定変更
LAN0	IPアドレス	192.168.0.1	○
	ネットマスク	24（255.255.255.0）	○
	セカンダリIPアドレス	なし	×
	DHCPサーバ機能	使用しない	×
	NAT機能	使用しない	×
	ダイナミックルーティング ・RIP送信 ・RIP受信	 RIP-V1を使用する RIP-V1を使用する	×
	転送レート	自動認識	○
LAN1	IPアドレス	192.168.1.1	○
	ネットマスク	24（255.255.255.0）	○
	セカンダリIPアドレス	なし	×
	DHCPサーバ機能	使用しない	×
	NAT機能	使用しない	×
	ダイナミックルーティング ・RIP送信 ・RIP受信	 RIP-V1を使用する RIP-V1を使用する	×



「詳細設定」で設定する

「かんたん設定」の場合とは異なり、「詳細設定」では、設定項目を個別に選択し、各項目を組み合わせて通信できる状態にします。詳細設定メニューを表示するには、NetVehicleのトップページで、画面上部の［詳細設定］アイコンをクリックします。
ここでは、既存の LAN-B に新規の LAN-A をネットワーク間接続し、静的に経路情報を設定する場合を例を説明します。



通信条件

［LAN-A 側］

- 転送レートは 10Mbps
- NetVehicle の LAN1 側の IP アドレス　：192.168.1.1
- ネットワークアドレス / ネットマスク　：192.168.1.0/24
- DHCP 機能を使用しない
- ルーティングプロトコルとして RIP-V1 を使用する
- NAT を使用しない

［LAN-B 側］

- 転送レートは 10Mbps
- NetVehicle の LAN0 側の IP アドレス　：192.168.0.1
- ネットワークアドレス / ネットマスク　：192.168.0.0/24
- DHCP 機能を使用しない
- インターネットにつながるルータ 1 と、事業所内のその他のネットワークにつながるルータ 2 が存在し、静的に経路情報を登録する
  ルータ 1 の IP アドレス　：192.168.0.5
  ルータ 2 の IP アドレス　：192.168.0.10
  LAN-C のネットワークアドレス / ネットマスク　：192.168.2.0/24
- NAT は使用しない

［その他の条件］

- 管理者パスワードを設定する
  新しいログインパスワード　：himitu
- 自動時刻設定にする
  タイムサーバ　：使用する
  サーバ設定　：設定する
  プロトコル　：TIME プロトコル
  タイムサーバのアドレス　：192.168.0.20

4

こんな事に気をつけて

文字入力フィールドには半角文字（0 〜 9、A 〜 Z、a 〜 z、および記号）だけを使用してください。ただし、空白文字、「 ”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

詳細設定で設定する

1. NetVehicle のトップページで詳細設定のアイコンをクリックします。

「詳細設定」ページが表示されます。

詳細設定で LAN0 情報を設定する

2. 詳細設定メニューで「LAN0 情報」をクリックします。

「LAN0 情報設定」ページが表示されます。

3. 以下の項目を指定します。

［IP アドレス］

- IP アドレス →指定する
- IP アドレス → 192.168.0.1
- ネットマスク → 24
- ブロードキャストアドレス →ネットワークアドレス＋オール 1

［IPアドレス］

IPアドレス	○ DHCPで自動的に取得する		
	⊙ 指定する		
		IPアドレス	192 . 168 . 0 . 1
		ネットマスク	24 (255.255.255.0)
		ブロードキャストアドレス	ネットワークアドレス +オール1

［ダイナミックルーティング機能］

- RIP 送信 → V1 で送信する
- RIP 受信 → V1 を受信する

［ダイナミックルーティング機能］

RIP送信	○ 送信しない ⊙ V1で送信する ○ V2で送信する
RIP受信	○ 受信しない ⊙ V1を受信する ○ V2を受信する

［NAT 情報］

- NAT の使用 →使用しない

［NAT情報］

NATの使用	⊙ 使用しない ○ NAT ○ マルチNAT ※NATの使用とDHCPリレーサービスの併用はできません

必要に応じて上記以外の項目を設定します。

4. ［スタティックルーティング情報一覧］［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。
［ルーティング情報設定］ページが表示されます。

5. 以下の項目を設定します。

- ネットワーク →ネットワーク指定
- 宛先 IP アドレス → 192.168.2.0
- 宛先ネットマスク → 24
- 中継ルータアドレス → 192.168.0.10
- メトリック値 → 1

4

6. ［更新］ボタンをクリックします。

「LAN0 情報設定」ページに戻ります。

7. ［スタティックルーティング情報一覧］で［追加］ボタンをクリックします。

［ルーティング情報設定］ページが表示されます。

8. 以下の項目を設定します。

- ネットワーク →デフォルトルート
- 中継ルータアドレス → 192.168.0.5

9. ［更新］ボタンをクリックします。

「LAN0 情報設定」ページに戻ります。

10. ［更新］ボタンをクリックします。

詳細設定で LAN1 情報を設定する

11. 詳細設定メニューで「LAN1 情報」をクリックします。

「LAN1 情報設定」ページが表示されます。

12. 以下の項目を指定します。

［IP アドレス］

- IP アドレス →指定する
- IP アドレス → 192.168.1.1
- ネットマスク → 24（255.255.255.0）
- ブロードキャストアドレス →ネットワークアドレス＋オール 1

[IPアドレス]

IPアドレス	○ DHCPで自動的に取得する ◉ 指定する	
	IPアドレス	192 . 168 . 1 . 1
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス＋オール1

［NAT 情報］

- NAT の使用 →使用しない

[NAT情報]

NATの使用	◉ 使用しない ○ NAT ○ マルチNAT ※NATの使用とDHCPリレーサービスの併用はできません

必要に応じて上記以外の項目を設定します。

13. ［更新］ボタンをクリックします。

14. ［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

管理者パスワードを設定することを強く推奨します。設定しない場合、ネットワーク上の誰からでもアクセスできるため非常に危険です。

管理者用パスワードを設定する

15. 詳細設定メニューで「パスワード情報」をクリックします。

「パスワード情報設定」ページが表示されます。

16. 以下の項目を指定します。

- 新しいログインパスワード　→ himitu
- ログインパスワードの確認　→ himitu

新しいログインパスワード	
ログインパスワードの確認	

17. ［更新］ボタンをクリックします。

「ログインパスワードを更新しました。以降の処理では、更新した情報を有効なものとします。」というメッセージが表示されます。

自動時刻設定の情報を設定する

18. 詳細設定メニューで「装置情報」をクリックします。

「装置情報設定」ページが表示されます。

19. ［タイムサーバ情報］で以下の項目を指定します。

- タイムサーバ　→ 使用する
- サーバ設定　→ 設定する
- プロトコル　→ TIME プロトコル（使用するプロトコルを選択）
- タイムサーバ IP アドレス　→ 192.168.0.20（タイムサーバの IP アドレス）
- 自動時刻設定間隔　→ 1 日（タイムサーバから情報を取得する間隔）
  日：　0 ～ 10
  時間：0 ～ 240

［タイムサーバ情報］

タイムサーバ	○ 使用しない ◉ 使用する
サーバ設定	○ DHCPで取得する ※DHCPクライアントの設定が必要です。 ◉ 設定する プロトコル：◉ TIMEプロトコル ○ SNTP タイムサーバIPアドレス：192 . 168 . 0 . 20
自動時刻設定間隔	1 日

20. ［更新］ボタンをクリックします。

21. ［設定反映］ボタンをクリックします。

設定した内容が有効になります。



TIME プロトコル、SNTPって？

TIME プロトコル（RFC868）はネットワーク上で時刻情報を配布するプロトコルです。SNTP（Simple Network Time Protocol、RFC1361、RFC1769）はNTP（NetworkTime Protocol）のサブセットで、パソコンなど末端のクライアントマシンの時刻を同期させるのに適しています。



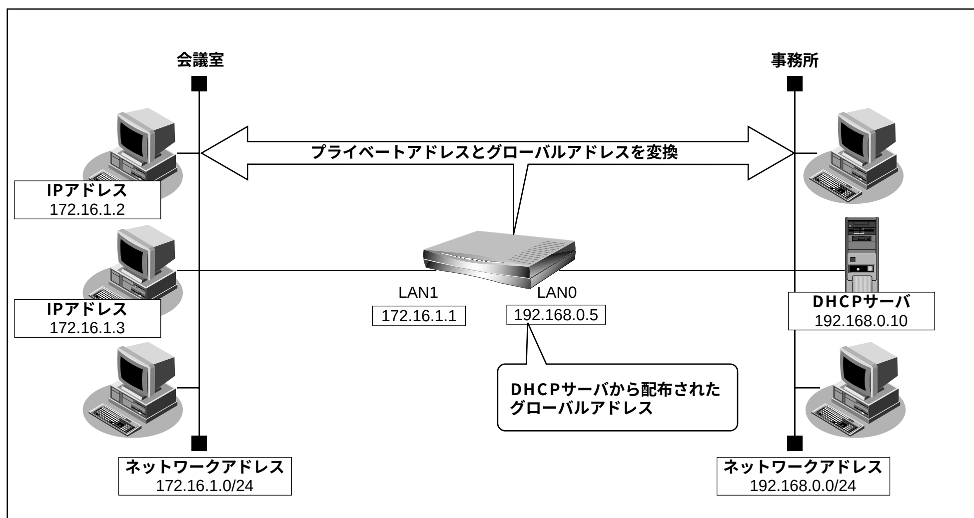
NetVehicle の便利な機能を活用する

この章では、
NetVehicle の便利な機能の活用方法について説明します。



マルチNAT機能（アドレス変換機能）を使う

NetVehicle はアドレス変換機能（NAT 機能）をサポートしています。NAT 機能は LAN 内に接続された複数台のパソコンで使用するプライベートアドレスをNetVehicleに割り当てたグローバルアドレスに変換する機能です。NAT 機能を使用すると限られた数のグローバルアドレスでそれ以上の数のパソコンを接続できます。また、LAN 内に接続されたパソコンのプライベートアドレスは外部から分からないため、他のネットワークからの不正なアクセスを遮断できます。





・プライベートアドレスとグローバルアドレスについて
プライベートアドレスとは、ユーザが自由に割り当てることができる IP アドレスです。
グローバルアドレスとは、インターネット上のホストを識別するために、InterNICなどのアドレス管理機構から割り当てられる世界で唯一の IP アドレスです。

・LAN どうしを接続する場合、場合によっては、両方プライベートアドレスとなることがあります。
NetVehicleでは便宜上、既存のLAN側のアドレスをグローバルアドレス、新規に構築するLAN側のアドレスをプライベートアドレスといいます。



こんな事に気をつけて

- **NetVehicleの 2 つのインタフェース（LAN0/LAN1）はいずれもアドレス変換機能を使用できます。しかし、一方のインタフェースのみ設定が有効です。2 つのインタフェースで同時に設定すると動作を保証できません。**
- **設定は、アドレス変換したい LAN とは反対側のインタフェースで行います。**
  - **・アドレス変換したい LAN のインタフェースが LAN1 の場合は LAN0 側に設定**
  - **・アドレス変換したい LAN のインタフェースが LAN0 の場合は LAN1 側に設定**

NAT 機能を使うと、すでに LAN を構築している場合も、プライベートアドレスを変更することなくインターネットに接続できるようになります。しかし、同時に接続できる台数は、割り当てられたグローバルアドレスの個数に限られます。これを解決するために、マルチ NAT 機能があります。マルチ NAT 機能を使うと、IP アドレス、ポート番号、プロトコル種別を使って、割り当てられたグローバルアドレスの個数以上のパソコンを接続できます。

マルチ NAT 機能とは、以下の 2 つの機能で構成されます。

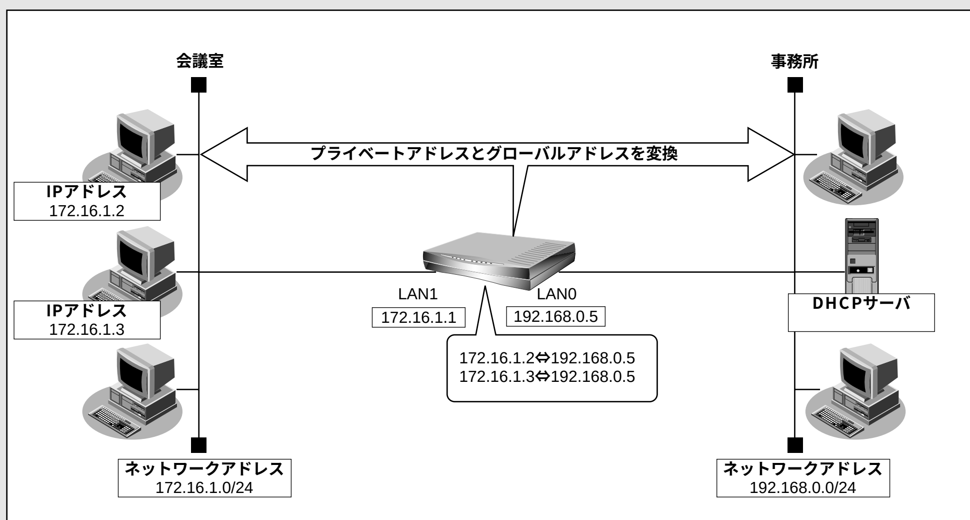
・動的 NAT
・静的 NAT

補足 カタログ等で説明するマルチ NAT 機能は基本 NAT、動的 NAT、静的 NAT の総称です。



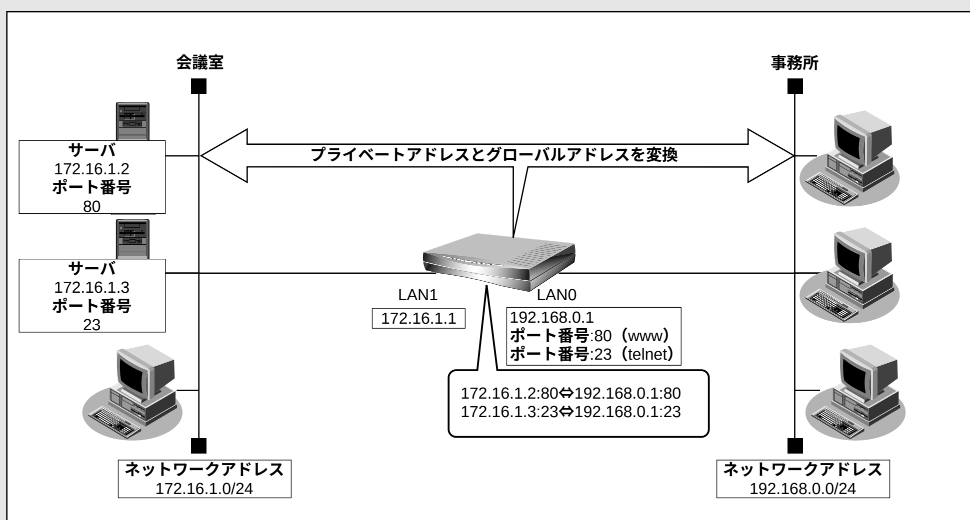
◆動的 NAT とは

基本 NAT 機能は、プライベートアドレスとグローバルアドレスを 1 対 1 に対応づけます。同時に接続できるパソコンの台数は 1 台です。「動的 NAT」を使えば、複数台のパソコンが同時に接続できます。



◆静的 NAT とは

基本 NAT 機能は、通信発生のたびに空いているグローバルアドレスを割り当てます。そのため、LAN 上の Web サーバを公開するような場合には適していません。「静的 NAT」を使えば、特定のパソコンやアプリケーションに同じ IP アドレス、ポート番号、プロトコル種別を割り当てるので、この問題が解決できます。



NAT機能の選択基準

ネットワーク環境および使用目的によって、適切なNAT機能を設定する必要があります。選択基準を以下に示します。

NAT機能が必要な場合

- プライベートLAN構築で、同時に複数台のパソコンから接続する場合
- LANに割り当てられたアドレス数を超える台数のパソコンを接続する場合
- 既存のネットワークのアドレスをそのまま使用する場合
- 自側のネットワークのアドレスを隠す場合

●基本NATで十分な場合

- ポート番号を変えたくない場合

●動的NATが必要な場合

- プライベートLAN構築で、同時に複数台のパソコンから接続する場合
- LANに割り当てられたアドレス数を超える台数のパソコンを接続する場合

●静的NATが必要な場合

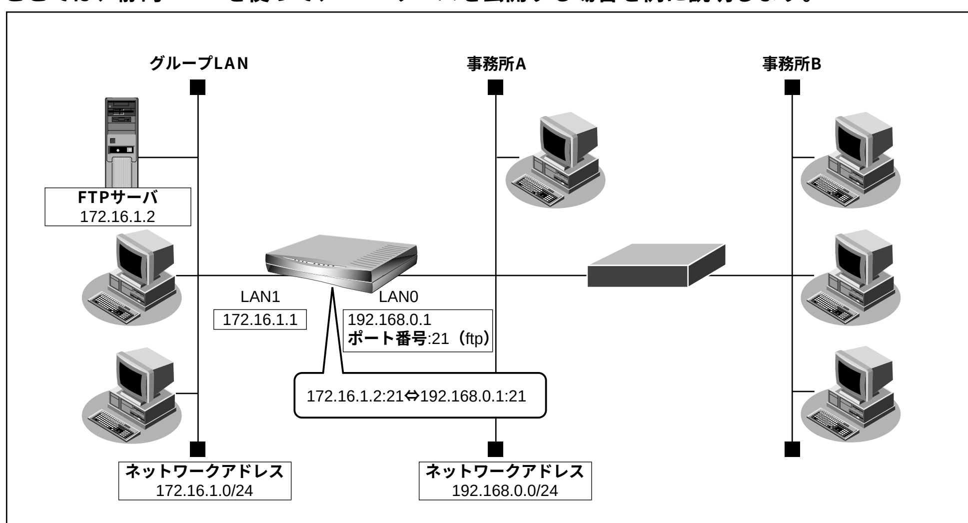
- 他のネットワークにサービスを公開する場合（WWWサーバ、FTPサーバなど）
- IPアドレスを意識して動作するアプリケーションを使用する場合

アプリケーションの中には、IPアドレスを意識して動作するものがあります。これらは、それぞれ独自のデータ形式をもち、データ中にIPアドレスを含むものがあります。
アドレスを変換する場合には、データ中のIPアドレスも意識しなくてはならないため、個別対応が必要となります。
NetVehicleは、すべてのアプリケーションに個別対応しているわけではありません。対応しているものは、特別な設定をせずに動作が可能となります。また、未対応のものでも、静的NAT機能を利用することで動作が可能になるものがあります。

補足 対応確認済みのアプリケーションについては、NetVehicleのサポートページを参照してください。

ネットワーク間接続でサーバを公開する

ここでは、静的 NAT を使って、FTP サーバを公開する場合を例に説明します。



通信条件

［事務所 A 側］

- 静的 NAT を使用する

［グループ LAN 側］

- IP アドレス ：172.16.1.1
- ネットワークアドレス／ネットマスク ：172.16.1.0/24
- FTP サーバの IP アドレス ：172.16.1.2

 こんな事に気をつけて

文字入力フィールドには半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「 ”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

詳細設定で静的 NAT 情報を設定する

1. **詳細設定メニューの「LAN0 情報」をクリックします。**
「LAN0 情報設定」ページが表示されます。

2. **［静的 NAT 情報一覧］で［追加］ボタンをクリックします。**
「静的 NAT 情報設定」ページが表示されます。

5

3. 以下の情報を設定します。

- プライベート IP 情報(IP アドレス)　→ 172.16.1.2
- プライベート IP 情報(ポート番号)　→ ftp
- グローバル IP 情報(IP アドレス)　→ 192.168.0.1
- グローバル IP 情報(ポート番号)　→ ftp
- プロトコル　→ tcp

プライベートIP情報	IPアドレス	172 . 16 . 1 . 2
	ポート番号	ftp (番号指定:) "その他"を選択時のみ有効です)
グローバルIP情報	IPアドレス	192 . 168 . 0 . 1
	ポート番号	ftp (番号指定:) "その他"を選択時のみ有効です)
プロトコル	tcp (番号指定:) "その他"を選択時のみ有効です)	

こんな事に気をつけて

動的 NAT と静的 NAT が混在する場合、動的 NAT で使用する IP アドレスと静的 NAT で使用する IP アドレスは重複しないようにしてください。

4. ［更新］ボタンをクリックします。

「LAN0 情報設定」ページに戻ります。

5. ［更新］ボタンをクリックします。

6. ［設定反映］ボタンをクリックします。

設定した内容が有効になります。



◆同時に接続できる台数

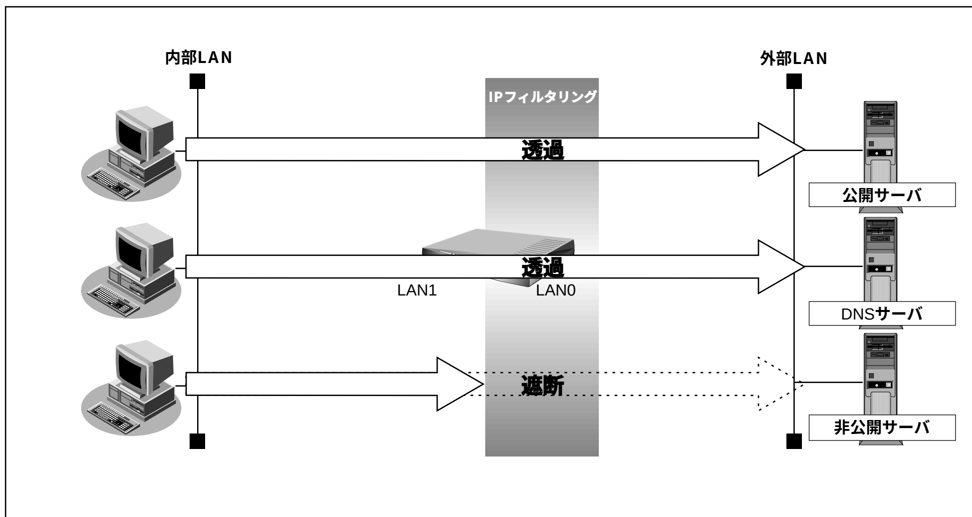
機能	同時接続台数および セッション数	備考
基本NAT機能	グローバルIPアドレス数 セッション数制限なし	割り当て時間内は外部からの通信も可能
動的NAT機能	接続台数制限なし 最大1024セッションまで	外部からの通信は不可能
静的NAT機能	最大64個まで割り当て可能 ＋動的NAT	プライベートアドレスとポートをグローバルアドレスとポートに割り当てできる 割り当てたアドレスとポートに関しては外部からの通信も可能

補足　NAT セキュリティは、" 高い " が初期値として選択されています。ftp や dns の要求した相手からの応答時には " 高い " を選択します。相手サーバが NAT を使用している場合など、要求先とは別のアドレスからの応答時には " 通常 " を選択してください。



IP フィルタリング機能を使う

NetVehicleを経由して送信または受信したパケットをIPアドレスとポート番号の組み合わせで制御することにより、ネットワークのセキュリティを向上させることができます。



ネットワークのセキュリティを向上させるには、次の要素について考える必要があります。

- ネットワークのセキュリティ方針
- ルータ以外の要素（ファイアウォール、ユーザ認証など）

NetVehicle は、パスワードを設定したり「IP フィルタリング機能」などを使って、ネットワークのセキュリティを向上させることができます。

 **こんな事に気をつけて**

- ProxyDNS を設定している場合、IP フィルタを設定しても効果はありません。
- NetVehicle などのルータでは、コンピュータウィルスの感染を防ぐことはできません。パソコン側でウィルス対策ソフトを使うなど、別の手段が必要です。



NAT 機能にも、セキュリティを向上させる効果があります。



NAT 機能→「マルチ NAT 機能（アドレス変換機能）を使う」（P.64）

接続形態に応じたセキュリティ方針を決める

データの流れには「外部から内部へ」、「内部から外部へ」という 2 つの方向があります。セキュリティを決める場合は、2 つの方向について考慮する必要があります。

●「外部から内部へ流れるデータ」に対するセキュリティ方針の例

- 非公開のサーバへのアクセスを防ぐ

●「内部から外部へ流れるデータ」に対するセキュリティ方針の例

- 外部へのアクセスを制限する
- 使用するアプリケーションを限定する

補足 IP フィルタリング機能は「外部から内部へ」流れるデータと「内部から外部へ」流れるデータに対して機能します。内部にあるパソコン間のデータ（LAN 内のデータ）に対しは機能しません。

こんな事に気をつけて

- IP フィルタリングの設定は外部側のインタフェースでのみ設定します。本書の例では LAN0 側を外部に接続しているので、すべて LAN0 側での設定になります。
- IP フィルタリングで WWW（ポート番号 80）でのアクセスを制限する設定を行った場合、外部の WWW ブラウザから設定ができなくなる場合があります。
- IP フィルタリングで DHCP（ポート番号 67,68）でのアクセスを制限する設定を行った場合、DHCP 機能が使用できなくなる場合があります。

IP フィルタリングの条件

IP フィルタリング機能では、以下の条件を設定することで、データの流れを制限できます。

- 動作
- プロトコル
- 送信元情報（IP アドレス／アドレスマスク／ポート番号）
- 宛先情報（IP アドレス／アドレスマスク／ポート番号）
- TCP 接続要求

動作	遮断	NetVehicleを介した通信が不可能
	透過	NetVehicleを介した通信が可能
プロトコル	すべて	IP通信はすべて対象
	UDP	UDP通信のみ対象
	TCP	TCP通信のみ対象
	ICMP	ICMP通信（PINGコマンド）のみ対象
	その他	上記以外の指定
送信元情報	IPアドレス	対象となるIPアドレス
宛先情報	アドレスマスク	対象範囲の指定
（項目共通）	ポート番号	対象となるポート番号
TCP接続要求	対象	すべて対象
	対象外	TCPコネクション確立パケットのみ対象外



◆TCP 接続要求とは

TCPプロトコルでのコネクション確立要求を、フィルタリングの対象にするかどうかを指定するものです。フィルタリングの動作に透過、プロトコルにTCPを指定した場合に有効です。TCPプロトコルはコネクション型であるため、コネクション確立要求を発行し、それに対する応答を受信することにより、コネクションを開設します。したがって、一方からのコネクションを禁止する場合でも、コネクション確立要求だけを遮断し、その他の応答や通常データなどを透過させるように設定しないと通信できません。

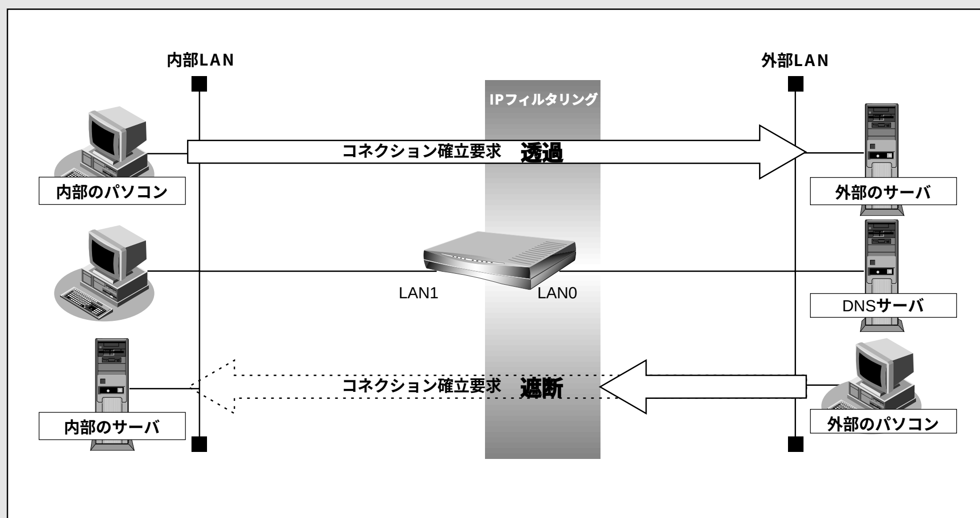
フィルタリングの動作に透過、TCP接続要求に対象外を指定した場合、コネクション確立要求だけを禁止する設定となり、対象となるアドレスからのコネクション接続を禁止できます。
次に、TCPパケットとフラグ設定について説明します。TCPパケット内にはSYNフラグとACKフラグの2つの制御フラグがあります。このフラグの組み合わせにより、TCPパケットの内容が分かります。以下、対応表を示します。

制御フラグ		TCPパケットの内容
SYN	ACK	
1	0	コネクションの確立要求
1	1	確立後の承認応答
0	1	確認応答、通常のデータ

この表から、制御フラグの組み合わせがSYN=1 ACK=0 の場合に、TCPパケットがコネクションの確立要求を行うことが分かります。つまり、IPパケットが禁止されているIPアドレスからの送信を禁止すれば、TCP/IPサービスのフィルタリングが行えます。

以下に、telnet（ポート番号23）の例を説明します。

・外部ネットワークからのコネクション確立要求は遮断
・内部ネットワークからのコネクション確立要求は透過



◆IP アドレスとアドレスマスクの決め方

フィルタリング条件の要素として「IPアドレス」と「アドレスマスク」があります。制御対象となるパケットはNetVehicleに届いたパケットのIPアドレスとアドレスマスクの論理積の結果が、指定したIPアドレスと一致したものに限ります。


アドレスマスクとは→「用語集」（P.138）

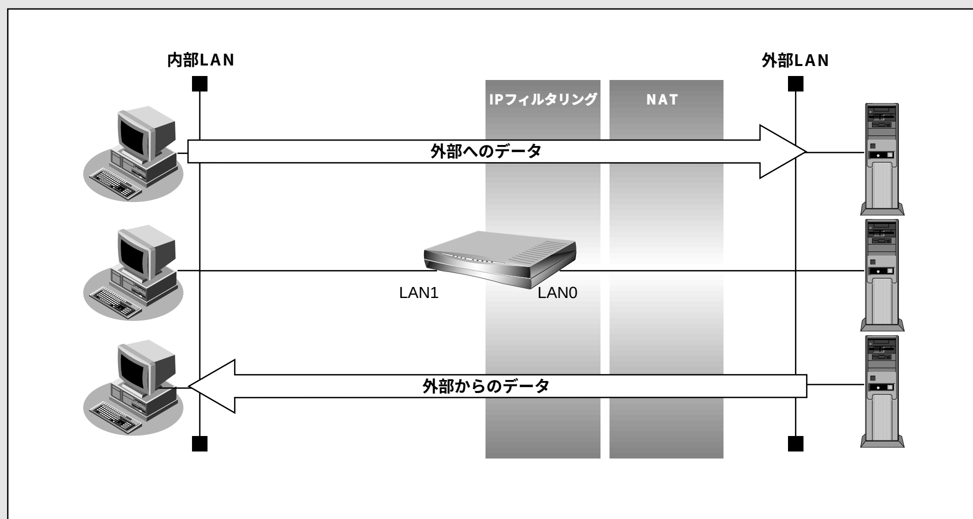
5



◆アドレス変換（NAT）機能利用時の IP フィルタリングのかかるタイミング

内部 LAN から外部 LAN に向かう場合は、アドレス変換でアドレスが変更される前にフィルタリング処理を通過します。また、外部 LAN から内部 LAN に向かう場合は、アドレス変換でアドレスが変更されたあとでフィルタリング処理を通過します。つまり、IP フィルタリングは「プライベートアドレス」を対象に行います。

NetVehicle の IP フィルタリングとアドレス変換の位置付けは以下のとおりです。



補足 IP フィルタリング機能とNAT機能を同時に使用する場合、回線切断時にNAT機能の情報が消えてしまうため、回線切断後に再度接続してもサーバからの応答が正しくアドレス変換されず、IP フィルタリング機能によってパケットは破棄されます。

フィルタリングの設計方針には大きく分類して以下の 2 つがあります。
A. 基本的にはパケットをすべて遮断し、特定の条件のものだけを透過させる。
B. 基本的にはパケットをすべて透過させ、特定のものだけを遮断する。

設計方針 A の例として、以下の設定例について説明します。
- **外部の特定サービスへのアクセスのみ許可する**
- **外部から特定サーバへのアクセスのみ許可する**

設計方針 B の例として、以下の設定例について説明します。
- **利用者が意図しない発信を防ぐ**
- **特定アドレスへのアクセスを禁止する**
- **回線が接続している時だけ許可する**

補足 TCP 接続要求の設定は、プロトコルに TCP またはすべてを指定した場合にだけ有効です。それ以外のプロトコルを指定した場合は無効となります。

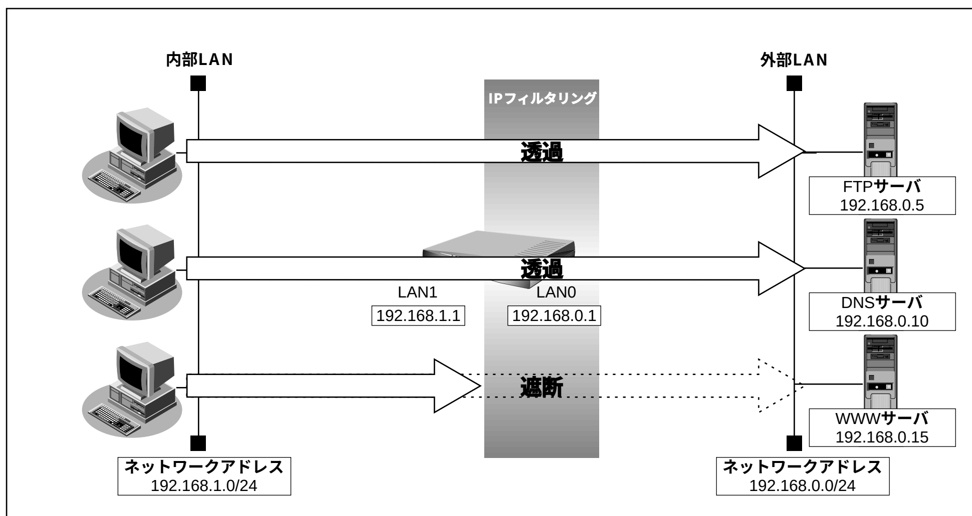
こんな事に気をつけて

フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。

外部の特定サービスへのアクセスのみ許可する

ここでは、一時的にLANを作成し、外部LANのすべてのFTPサーバへのアクセスのみを許可し、他のサーバへのアクセスは禁止する場合を例に説明します。ただし、アドレス情報を取り出すためにDNSサーバへのアクセスを許可する設定にします。

補足
- ftpでホスト名を指定する場合、DNSサーバに問い合わせが発生するため、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、ftpサービス以外でもドメイン名で指定されるとDNSサーバへの問い合わせが発生します。あらかじめ接続するftpサーバが決まっている場合は、NetVehicleのDNSサーバ機能を利用することによって、DNSサーバへの問い合わせを抑止することができます。
- NetVehicleはftp-data転送に関するフィルタリングルールを自動的に作成します。



●フィルタリング設計

- **内部LANのホスト（192.168.1.0/24）から外部LANのFTPサーバへのアクセスを許可**
- **内部LANのホスト（192.168.1.0/24）から外部LANへのDNSサーバへのアクセスを許可**
- **その他はすべて遮断**

●フィルタリングルール

- **FTPサーバへのアクセスを許可するには**
  （1）192.168.1.0/24の任意のポートから、任意のFTPサーバのポート21（ftp）へのTCPパケットを透過させる
  （2）（1）の応答パケットを透過させる
- **DNSの問い合わせを許可するには**
  （1）192.168.1.0/24の任意のポートからDNSサーバのポート53（domain）へのパケットを透過させる
  （2）（1）の応答パケットを透過させる
- **その他をすべて遮断するには**
  （1）すべてのパケットを遮断する

補足 このルールでは、passiveモードによるデータ転送はできません。

上記のフィルタリングルールの設定を行う場合を例に説明します。

こんな事に気をつけて

文字入力フィールドには半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

任意のFTPサーバのポート21へのTCPパケットを透過させる（内部LAN→外部LAN）

1. 詳細設定メニューの「LAN0 情報」をクリックします。

「LAN0 情報設定」ページが表示されます。

2. ［IP フィルタリング情報一覧］で［追加］ボタンをクリックします。

「IP フィルタリング情報設定」ページが表示されます。

3. ［IP フィルタリング情報］で以下の項目を指定します。

- 動作 →透過
- プロトコル → tcp
- 送信元情報（IP アドレス） → 192.168.1.0
- 送信元情報（アドレスマスク） → 24
- 送信元情報（ポート番号） →なにも設定しない
- 宛先情報（IP アドレス） →なにも設定しない
- 宛先情報（アドレスマスク） →なにも設定しない
- 宛先情報（ポート番号） → 21（ftp のポート番号）
- TCP 接続要求 →対象

[IPフィルタリング情報]

動作		◉ 透過 ○ 遮断
プロトコル		tcp （番号指定: ＿ “その他”を選択時のみ有効です）
送信元情報	IPアドレス	192 . 168 . 1 . 0
	アドレスマスク	24 (255.255.255.0)
	ポート番号[...]	
宛先情報	IPアドレス	. . .
	アドレスマスク	0 (0.0.0.0)
	ポート番号[...]	21
TCP接続要求		◉ 対象 ○ 対象外

4. ［更新］ボタンをクリックします。

「LAN0 情報設定」ページに戻ります。

FTP サーバからの TCP の応答パケットを透過させる（外部 LAN →内部 LAN）

5.　手順 2. ～ 4. の処理を繰り返し、以下の情報を設定します。

[IP フィルタリング情報]

- 動作　→透過
- プロトコル　→ tcp
- 送信元情報（IP アドレス）　→なにも設定しない
- 送信元情報（アドレスマスク）　→なにも設定しない
- 送信元情報（ポート番号）　→ 21（ftp のポート番号）
- 宛先情報（IP アドレス）　→ 192.168.1.0
- 宛先情報（アドレスマスク）　→ 24
- 宛先情報（ポート番号）　→なにも設定しない
- TCP 接続要求　→対象外

DNS サーバアドレスのポート 53 への UDP パケットを透過させる（内部 LAN →外部 LAN）

6.　手順 2. ～ 4. の処理を繰り返し、以下の情報を設定します。

[IP フィルタリング情報]

- 動作　→透過
- プロトコル　→ udp
- 送信元情報（IP アドレス）　→ 192.168.1.0
- 送信元情報（アドレスマスク）　→ 24
- 送信元情報（ポート番号）　→なにも設定しない
- 宛先情報（IP アドレス）　→ 192.168.0.10
- 宛先情報（アドレスマスク）　→ 32
- 宛先情報（ポート番号）　→ 53（domain のポート番号）
- TCP 接続要求　→対象

DNS の応答パケットを透過させる（外部 LAN →内部 LAN）

7.　手順 2. ～ 4. の処理を繰り返し、以下の情報を設定します。

[IP フィルタリング情報]

- 動作　→透過
- プロトコル　→ udp
- 送信元情報（IP アドレス）　→ 192.168.0.10
- 送信元情報（アドレスマスク）　→ 32
- 送信元情報（ポート番号）　→ 53（domain のポート番号）
- 宛先情報（IP アドレス）　→ 192.168.1.0
- 宛先情報（アドレスマスク）　→ 24
- 宛先情報（ポート番号）　→なにも設定しない
- TCP 接続要求　→対象

残りの通信はすべて遮断する

8. **手順 2. ～ 4. の処理を繰り返し、以下の情報を設定します。**

[IP フィルタリング情報]

- 動作 →遮断
- プロトコル →すべて
- 送信元情報（IP アドレス） →なにも設定しない
- 送信元情報（アドレスマスク） →なにも設定しない
- 送信元情報（ポート番号） →なにも設定しない
- 宛先情報（IP アドレス） →なにも設定しない
- 宛先情報（アドレスマスク） →なにも設定しない
- 宛先情報（ポート番号） →なにも設定しない
- TCP 接続要求 →対象

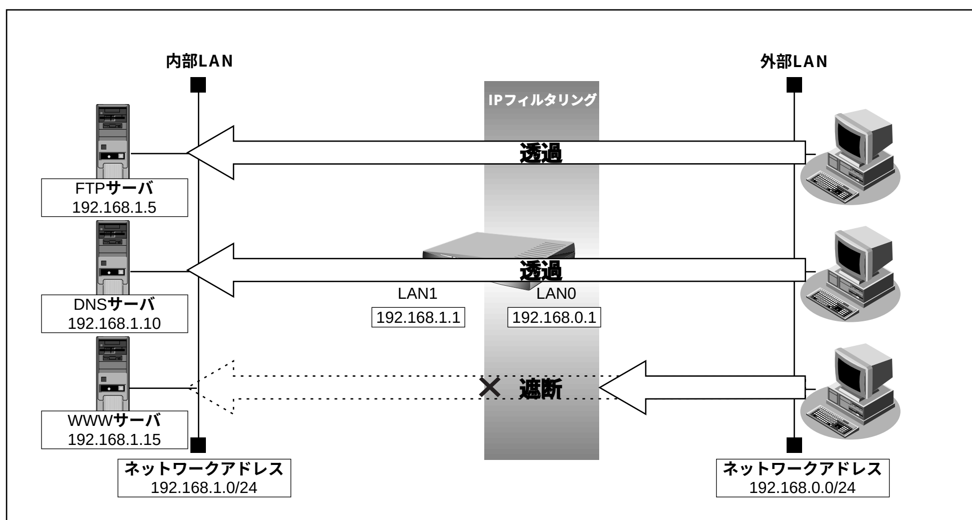
9. **［更新］ボタンをクリックします。**

10. **［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

外部から特定サーバへのアクセスのみ許可する

ここでは、内部LANの特定サーバのみを許可し、他のサーバへのアクセスは禁止する場合を例に説明します。ただし、アドレス情報を取り出すDNSサーバへのアクセスを許可する設定にします。



5

●フィルタリング設計

- **内部LANのホスト（192.168.1.5/32）をFTPサーバとして利用することを許可**
- **内部LANのネットワークへのDNSサーバへの問い合わせは許可**
- **その他はすべて遮断**

補足 ・ftpでホスト名を指定する場合、DNSサーバに問い合わせが発生するため、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、ftpサービス以外でもドメイン名で指定されるとDNSサーバへの問い合わせが発生します。あらかじめ接続するftpサーバが決まっている場合は、NetVehicleのDNSサーバ機能を利用することによって、DNSサーバへの問い合わせを抑止することができます。

・NetVehicleはftp-data転送に関するフィルタリングルールを自動的に作成します。

●フィルタリングルール

- **FTPサーバとしての利用を許可するには**
  （1）192.168.1.5/32のポート21（ftp）へのTCPパケットを透過させる
  （2）（1）の応答パケットを透過させる
- **DNSサーバへのアクセスを許可するには**
  （1）192.168.0.0/24の任意のポートからDNSサーバのポート53（domain）へのUDPパケットを透過させる
  （2）（1）の応答パケットを透過させる
- **その他をすべて遮断するには**
  （1）すべてのパケットを遮断する

補足 このルールでは、passiveモードによるデータ転送はできません。

上記のフィルタリングルールの設定を行う場合を例に説明します。

こんな事に気をつけて

文字入力フィールドには半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

FTP サーバのポート 21 へのパケットを透過させる（外部 LAN →内部 LAN）

1. 詳細設定メニューの「LAN0 情報」をクリックします。

「LAN0 情報設定」ページが表示されます。

2. [IP フィルタリング情報一覧］で［追加］ボタンをクリックします。

「IP フィルタリング情報設定」ページが表示されます。

3. [IP フィルタリング情報］で以下の項目を指定します。

- 動作 →透過
- プロトコル → tcp
- 送信元情報（IP アドレス） → 192.168.0.0
- 送信元情報（アドレスマスク） → 24
- 送信元情報（ポート番号） →なにも設定しない
- 宛先情報（IP アドレス） → 192.168.1.5
- 宛先情報（アドレスマスク） → 32
- 宛先情報（ポート番号） → 21（ftp のポート番号）
- TCP 接続要求 →対象

[IPフィルタリング情報]

動作		⦿ 透過 ○ 遮断
プロトコル		tcp （番号指定: ＂その他＂を選択時のみ有効です）
送信元情報	IPアドレス	192 .168 .0 .0
	アドレスマスク	24 (255.255.255.0)
	ポート番号[...]	
宛先情報	IPアドレス	192 .168 .1 .5
	アドレスマスク	32 (255.255.255.255)
	ポート番号[...]	21
TCP接続要求		⦿ 対象 ○ 対象外

4. [更新］ボタンをクリックします。

「LAN0 情報設定」ページに戻ります。

TCP の応答パケットを透過させる（内部 LAN →外部 LAN）

5. **手順 2. ～ 4. の処理を繰り返し、以下の情報を設定します。**

[IP フィルタリング情報]

- 動作 →透過
- プロトコル → tcp
- 送信元情報（IP アドレス） → 192.168.1.5
- 送信元情報（アドレスマスク） → 32
- 送信元情報（ポート番号） → 21（ftp のポート番号）
- 宛先情報（IP アドレス） → 192.168.0.0
- 宛先情報（アドレスマスク） → 24
- 宛先情報（ポート番号） →なにも指定しない
- TCP 接続要求 →対象外

DNS サーバアドレスのポート 53 への UDP パケットを透過させる（外部 LAN →内部 LAN）

6. **手順 2. ～ 4. の処理を繰り返し、以下の情報を設定します。**

[IP フィルタリング情報]

- 動作 →透過
- プロトコル → udp
- 送信元情報（IP アドレス） → 192.168.0.0
- 送信元情報（アドレスマスク） → 24
- 送信元情報（ポート番号） →なにも設定しない
- 宛先情報（IP アドレス） → 192.168.1.10
- 宛先情報（アドレスマスク） → 32
- 宛先情報（ポート番号） → 53（domain のポート番号）
- TCP 接続要求 →対象

DNS の応答パケットを透過させる（内部 LAN →外部 LAN）

7. **手順 2. ～ 4. の処理を繰り返し、以下の情報を設定します。**

[IP フィルタリング情報]

- 動作 →透過
- プロトコル → udp
- 送信元情報（IP アドレス） → 192.168.1.10
- 送信元情報（アドレスマスク） → 32
- 送信元情報（ポート番号） → 53（domain のポート番号）
- 宛先情報（IP アドレス） → 192.168.0.0
- 宛先情報（アドレスマスク） → 24
- 宛先情報（ポート番号） →なにも設定しない
- TCP 接続要求 →対象

残りの通信はすべて遮断する

8. **手順 2. ～ 4. の処理を繰り返し、以下の情報を設定します。**

［IP フィルタリング情報］

- 動作 →遮断
- プロトコル →すべて
- 送信元情報（IP アドレス） →なにも設定しない
- 送信元情報（アドレスマスク） →なにも設定しない
- 送信元情報（ポート番号） →なにも設定しない
- 宛先情報（IP アドレス） →なにも設定しない
- 宛先情報（アドレスマスク） →なにも設定しない
- 宛先情報（ポート番号） →なにも設定しない
- TCP 接続要求 →対象

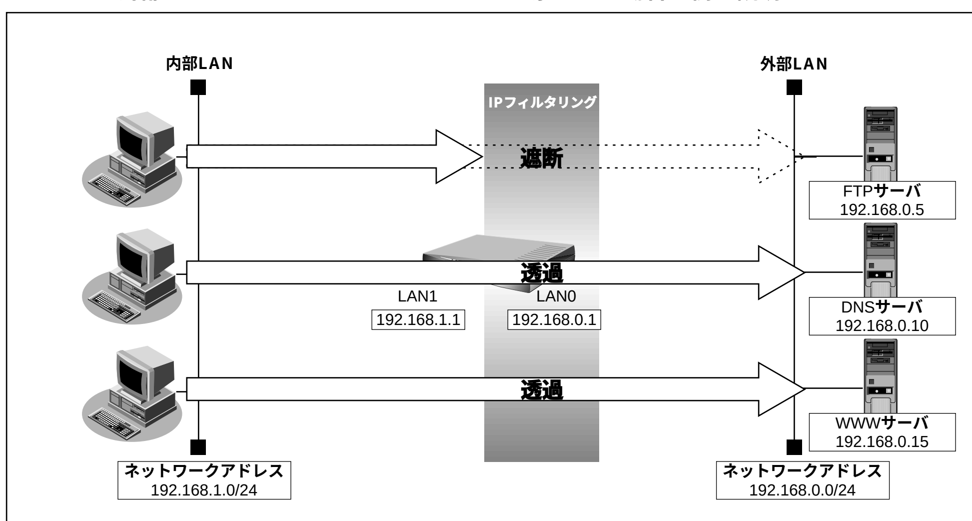
9. **［更新］ボタンをクリックします。**

10. **［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

特定サーバへのアクセスを禁止する

ここでは、外部 LAN の FTP サーバへのアクセスを禁止する場合を例に説明します。



●フィルタリング設定

- 内部 LAN のホスト（192.168.1.0/24）から外部 LAN の FTP サーバ（192.168.0.5）へのアクセスを禁止

●フィルタリングルール

- FTP サーバへのアクセスを禁止するには

（1）192.168.1.0/24 から 192.168.0.5 のポート 21（ftp）への TCP パケットを遮断する

5

上記のフィルタリングルールの設定を行う場合を例に説明します。

こんな事に気をつけて

文字入力フィールドには半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

特定サーバ（192.168.0.5）へのアクセスを禁止する（内部 LAN →外部 LAN）

1. **詳細設定メニューの「LAN0 情報」をクリックします。**

「LAN0 情報設定」ページが表示されます。

2. **[IP フィルタリング情報一覧］で［追加］ボタンをクリックします。**

「IP フィルタリング情報設定」ページが表示されます。

3. **[IP フィルタリング情報］で以下の項目を指定します。**

- 動作 →遮断
- プロトコル → tcp
- 送信元情報（IP アドレス） → 192.168.1.0
- 送信元情報（アドレスマスク） → 24
- 送信元情報（ポート番号） →なにも設定しない
- 宛先情報（IP アドレス） → 192.168.0.5
- 宛先情報（アドレスマスク） → 32
- 宛先情報（ポート番号） → 21
- TCP 接続要求 →対象

[IPフィルタリング情報]

動作		○ 透過 ◉ 遮断
プロトコル		tcp（番号指定: ）"その他"を選択時のみ有効です）
送信元情報	IPアドレス	192 .168 .1 .0
	アドレスマスク	24 (255.255.255.0)
	ポート番号[...]	
宛先情報	IPアドレス	192 .168 .0 .5
	アドレスマスク	32 (255.255.255.255)
	ポート番号[...]	21
TCP接続要求		◉ 対象 ○ 対象外

4. **[更新］ボタンをクリックします。**

「LAN0 情報設定」ページに戻ります。

5. **[更新］ボタンをクリックします。**

6. **[設定反映］ボタンをクリックします。**

設定した内容が有効になります。



DHCP 機能を使う

NetVehicle の DHCP 機能には、以下のような機能があります。

- DHCP サーバ機能
- DHCP スタティック機能
- DHCP クライアント機能
- DHCP リレーエージェント機能

NetVehicle では、それぞれのインタフェース（LAN0、LAN1）で DHCP 機能が使用できます。なお、組み合わせによっては正常に通信できなくなるので、ご注意ください。以下に DHCP 機能の組み合わせ一覧を示します。

LAN0/LAN1 インタフェースの DHCP 機能の組合せ

		LAN1			
		サーバ（スタティック）	クライアント	リレーエージェント	DHCP機能を使用しない
LAN0	サーバ（スタティック）	○	○	×	○
	クライアント	○	○	○	○
	リレーエージェント	×	○	×	○
	DHCP機能を使用しない	○	○	○	○

○：動作可能な組み合わせ　　×：動作不可能な組み合わせ



こんな事に気をつけて

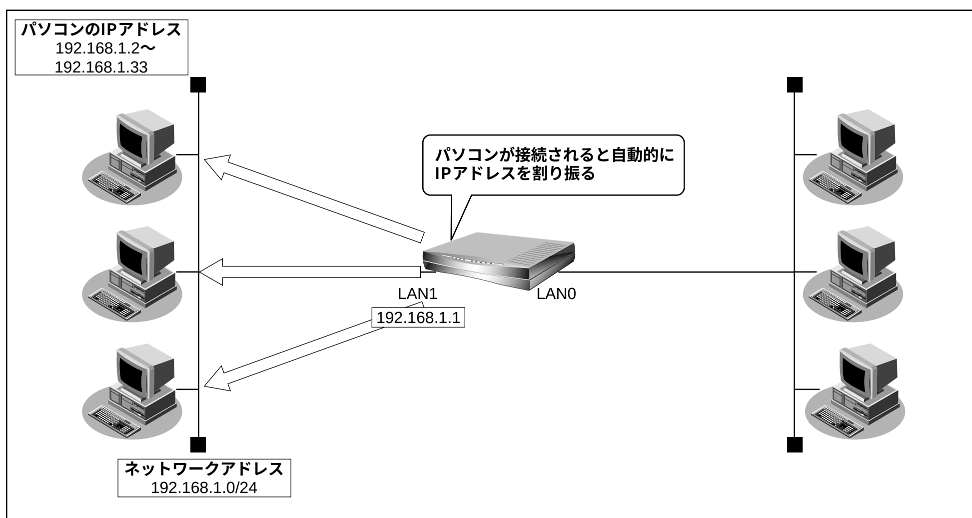
1 つのインタフェースでは、1 つの機能だけ動作します。同時に複数の機能は動作しません。

5

DHCP サーバ機能

DHCP サーバ機能は、LAN 内のパソコンに対して IP アドレスの自動割当てを行う機能です。IP アドレスは重複が許されず、また、パソコンが増えるたびに管理者が設定する必要がありますが、この機能を利用すると DHCP クライアント機能を持つパソコンには IP アドレスの設定が不要になり、管理者の手間を大幅に省くことができます。
NetVehicle の DHCP サーバ機能は、以下の情報を広報することができます。

・IP アドレス
・ネットマスク
・リース期間
・デフォルトルータの IP アドレス
・DNS サーバの IP アドレス
・ドメイン名



ここでは、DHCP サーバ機能を使う場合を例に説明します。
通信条件

- NetVehicle の IP アドレス　：192.168.1.1
- パソコンに割り当てる IP アドレス　：192.168.1.2 ～ 192.168.1.33
- パソコンに割り当てる IP アドレス数　：32
- ネットワークアドレス / ネットマスク　：192.168.1.0/24
- DHCP サーバ機能を使用する

 こんな事に気をつけて

- 文字入力フィールドには半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「 ”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
- NetVehicle の DHCP サーバ機能は、DHCP リレーエージェントのサーバにはなれません。

詳細設定で DHCP サーバ機能を設定する

1. **詳細設定メニューで「LAN1 情報」をクリックします。**

「LAN1 情報設定」ページが表示されます。

2. **［IP アドレス］で以下の項目を指定します。**

- IP アドレス →指定する
- IP アドレス → 192.168.1.1
- ネットマスク → 24
- ブロードキャストアドレス →ネットワークアドレス + オール 1

3. **［DHCP 機能］で［修正］ボタンをクリックします。**

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら、［OK］ボタンをクリックします。

「DHCP 情報設定」ページが表示されます。

4. **［DHCP 機能］で以下の項目を指定します。**

- LAN1 →サーバ機能を使用する
- 割当て先頭 IP アドレス → 192.168.1.2
- 割当てアドレス数 → 32

補足 DHCP サーバ機能で割り当てることのできる最大数は 253 です。

必要に応じて上記以外の項目を設定します。

5. **［更新］ボタンをクリックします。**

「LAN1 情報設定」ページに戻ります。

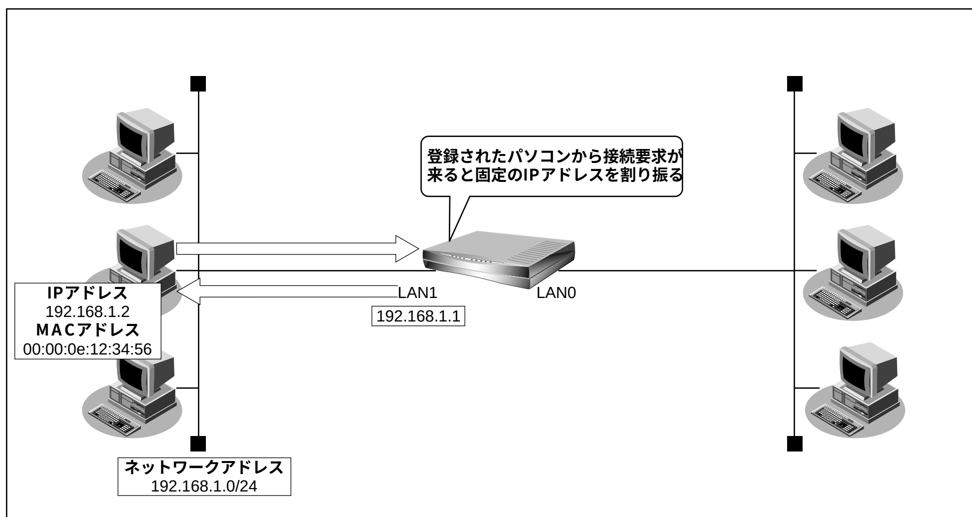
6. **［更新］ボタンをクリックします。**

7. **［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

DHCP スタティック機能

DHCP サーバは空いているIP アドレスを一定期間（またはパソコンが返却するまで） 割り当て、不要になったIP アドレスは自動的に再利用します。このため、パソコンのIP アドレスが変わることがあります。NetVehicle では、IP アドレスと MAC アドレスを対応づけることによって、登録された接続機器からDHCP要求が発行されると､常に同じIPアドレスを割り当てることができます｡これを｢DHCPスタティック機能」といいます。
ここでは、DHCP スタティック機能を使う場合を例に説明します。



DHCP スタティック機能を利用する場合は、ホストデータベース情報にIP アドレスと MAC アドレスを設定します。

補足
・MAC アドレスとは、LAN 機器に設定されていて世界中で重複されないように管理されている固有のアドレスです。
・NetVehicle がサポートしている「IP フィルタリング機能」､「静的 NAT 機能」などはパソコンのIP アドレスが固定されていないと使いにくい場合があります。これらの機能と DHCP サーバ機能の併用を実現するために、「DHCP スタティック機能」をサポートしています。

通信条件
- **ネットワークアドレス / ネットマスク　　：192.168.1.0/24**
- **IP アドレスを固定したいパソコンの MAC アドレス　　：00:00:0e:12:34:56**
- **割当て IP アドレス　　：192.168.1.2**
- **DHCP サーバ機能を使用する**

こんな事に気をつけて

- **詳細設定の「LAN0 情報」､「LAN1 情報」で DHCP サーバ機能を使用する設定をしていない場合は、DHCP スタティック機能の設定は有効になりません。**
- **文字入力フィールドには半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「 ”｣、｢<｣、｢>｣、｢&｣、｢%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。**

詳細設定で DHCP スタティック機能を設定する

1. **詳細設定メニューで「ホストデータベース情報」をクリックします。**
「ホストデータベース情報」ページが表示されます。

2. **未設定の欄の［修正］ボタンをクリックします。**
「ホストデータベース情報設定」ページが表示されます。

3. **以下の項目を設定します。**

- IP アドレス → 192.168.1.2
- MAC アドレス → 00:00:0e:12:34:56

補足 ホストデータベース情報は「リモートパワーオン機能」、「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。

ホスト名	
IPアドレス	192 . 168 . 1 . 2
MACアドレス	00 : 00 : 0e : 12 : 34 : 56
リモート電源制御	◉ 対象 ○ 対象外

必要に応じて上記以外の項目を設定します。

4. **［更新］ボタンをクリックします。**
「ホストデータベース情報」ページに戻ります。

5. **［設定反映］ボタンをクリックします。**
設定した内容が有効になります。

補足 DHCP スタティック機能で設定できるホストの最大数は 64 です。

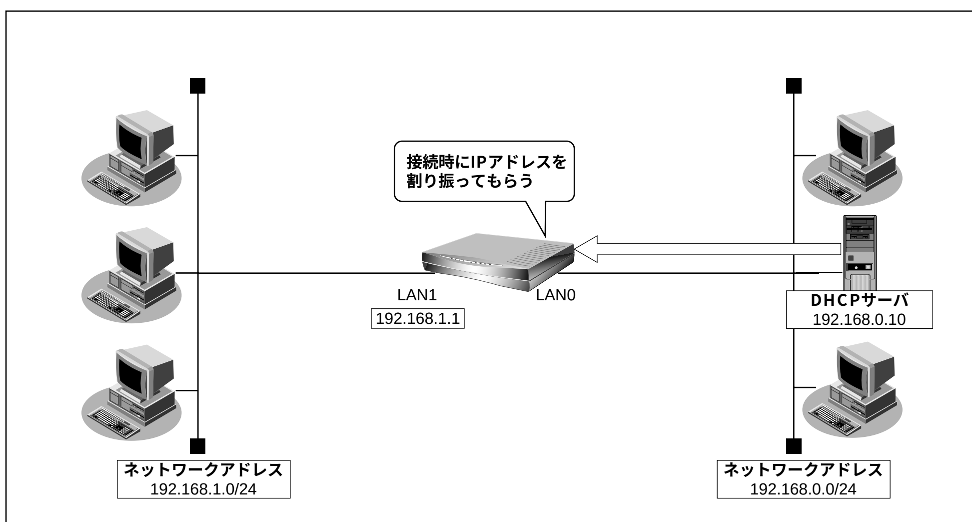
5

DHCP クライアント機能

DHCP クライアント機能は、DHCP サーバから IP アドレスなどの情報を取得する機能です。使用する場合は DHCP サーバが動作している LAN に接続する必要があります。利用者は、IP アドレスを意識することなくネットワークを利用できます。
NetVehicle の DHCP クライアント機能は以下の情報を受け取って動作できます。

- **IP アドレス**
- **ネットマスク**
- **リース期間**
- **デフォルトルータの IP アドレス**
- **DNS サーバの IP アドレス**
- **TIME サーバの IP アドレス**
- **NTP サーバの IP アドレス**

ここでは、DHCP クライアント機能を使う場合を例に説明します。



通信条件

- **NetVehicle の IP アドレス　　　：DHCP サーバから取得する**

 **こんな事に気をつけて**

文字入力フィールドには半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「 ”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

詳細設定で DHCP クライアント機能を設定する

1. **詳細設定メニューで「LAN0 情報」をクリックします。**

「LAN0 情報設定」ページが表示されます。

2. **［IP アドレス］で以下の項目を指定します。**

- IP アドレス　　　　　→ DHCP で自動的に取得する

［IPアドレス］

IPアドレス	◉ DHCPで自動的に取得する ○ 指定する
	IPアドレス：192.168.0.1
	ネットマスク：24 (255.255.255.0)
	ブロードキャストアドレス：ネットワークアドレス＋オール1
	※DHCPサーバ機能使用時、IPアドレスを変更する場合はDHCPサーバ機能の“割当て先頭IPアドレス”も確認してください。

3. **［更新］ボタンをクリックします。**

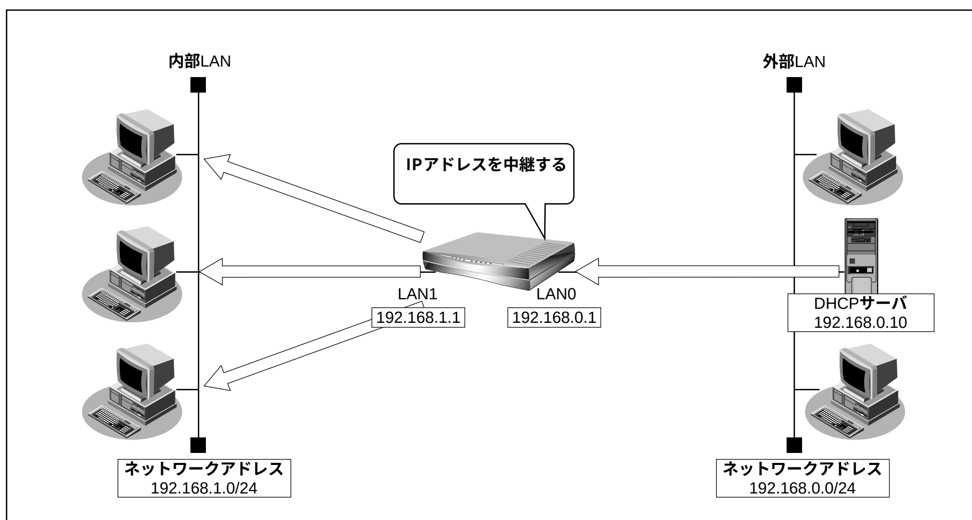
4. **［設定反映］ボタンをクリックします。**

設定した内容が　有効になります。

DHCP リレーエージェント機能

DHCPリレーエージェントは遠隔地にあるDHCPサーバが配布する情報を中継する機能です。この機能を利用することで、遠隔地の別のネットワークにDHCPサーバが存在する場合も同じように情報を獲得することができます。

ここでは、DHCP リレーエージェントを使う場合を例に説明します。



通信条件

［内部 LAN 側］

- NetVehicle の IP アドレス　　：192.168.1.1
- DHCP リレーエージェント機能を使用する

5

［外部 LAN 側］
- NetVehicle の IP アドレス　：192.168.0.1
- DHCP サーバ　：192.168.0.10

補足　DHCP リレーエージェント機能を使うときは、NAT 機能を使用できません。

こんな事に気をつけて

文字入力フィールドには半角文字（0 〜 9、A 〜 Z、a 〜 z、および記号）だけを使用してください。ただし、空白文字、「 ”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

詳細設定で DHCP リレーエージェント機能を設定する

ここでは、LAN1 を使用した場合を例に説明します。LAN0 の場合も同様の手順で設定できます。

1. 詳細設定メニューで「LAN1 情報」をクリックします。

「LAN1 情報設定」ページが表示されます。

2. ［DHCP 機能］で［修正］ボタンをクリックします。

「DHCP 情報設定」ページが表示されます。

3. ［DHCP 機能］で以下の項目を設定します。

- LAN1　→ リレー機能を使用する
- DHCP サーバ IP アドレス → 192.168.0.10

使用しない
リレー機能を使用する
DHCPサーバIPアドレス 192 . 168 . 0 . 10
サーバ機能を使用する
割当て先頭IPアドレス 192 . 168 . 1 . 2
割当てアドレス数 253
LAN1

4. ［更新］ボタンをクリックします。

「LAN1 情報設定」ページに戻ります。

5. ［更新］ボタンをクリックします。

6. ［設定反映］ボタンをクリックします。

設定した内容が有効になります。



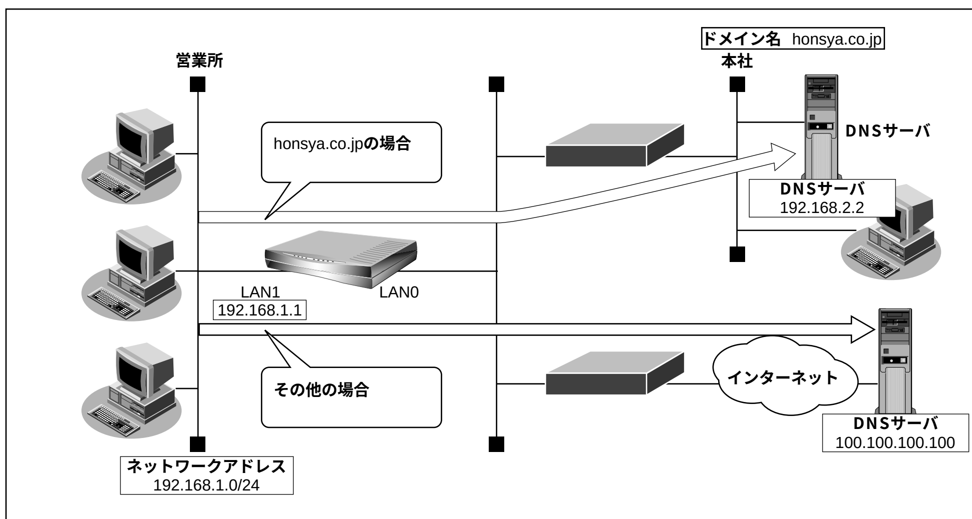
DNS サーバを使う（ProxyDNS）

NetVehicle の ProxyDNS には、以下のような機能があります。

- DNS サーバの自動切り替え機能
- DNS サーバ機能

DNS サーバの自動切り替え機能（順引き）

ProxyDNS は、パソコン側で NetVehicle の IP アドレスを DNS サーバの IP アドレスとして登録するだけで、ドメインごとに使用したい DNS サーバを切り替えて中継できます。ここでは、順引きの場合を例に説明します。



通信条件

- 会社の DNS サーバを使う場合
  使用するドメイン　　　　：honsya.co.jp
  DNS サーバの IP アドレス：192.168.2.2
- インターネット上の DNS サーバを使う場合
  使用するドメイン　　　　：honsya.co.jp 以外
  DNS サーバの IP アドレス：100.100.100.100

パソコン側の設定を確認する

1. **パソコン側が DHCP クライアントかどうか確認します。**
DHCP クライアントでない場合は設定します。


ProxyDNS の設定をする→「Q&A　Q17 」（P.145 ）

こんな事に気をつけて

文字入力フィールドには半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

詳細設定で ProxyDNS 情報を設定する

1. 詳細設定メニューで「ProxyDNS 情報」をクリックします。

「ProxyDNS 情報」ページが表示されます。

2. ［順引き情報一覧］で［追加］ボタンをクリックします。

「ProxyDNS 情報設定（順引き）」ページが表示されます。

3. 以下の項目を指定します。

- ドメイン名　→＊.honsya.co.jp
- 動作　→設定した DNS サーバへ問い合わせる
- DNS サーバアドレス　→ 192.168.2.2

ドメイン名	*. honsya. co. jp
動作	○ 廃棄する ◉ 設定したDNSサーバへ問い合わせる DNSサーバアドレス 192 .168 .2 .2

4. ［更新］ボタンをクリックします。

「ProxyDNS 情報」ページに戻ります。

5. 手順 2.～4. の処理を繰り返し、以下の情報を設定します。

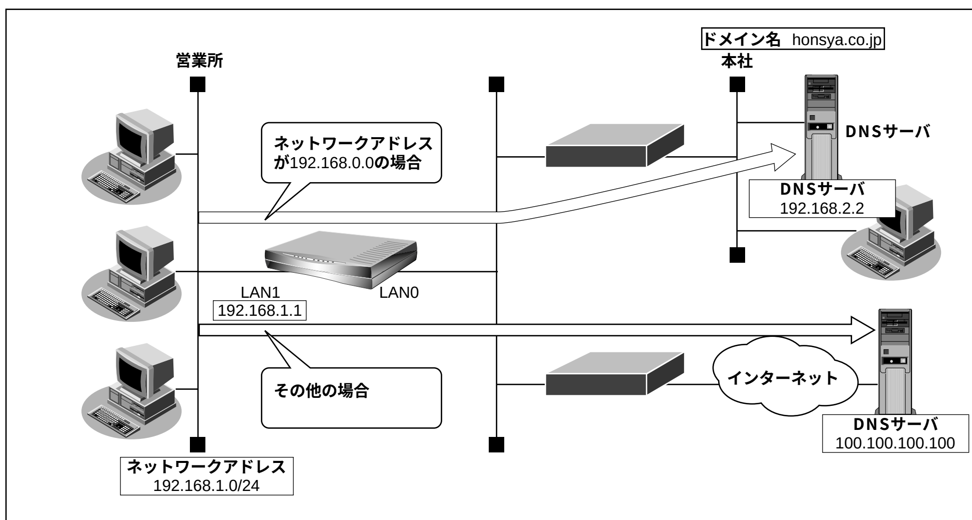
- ドメイン名　→＊
- 動作　→設定した DNS サーバへ問い合わせる
- DNS サーバアドレス　→ 100.100.100.100

6. ［設定反映］ボタンをクリックします。

設定した内容が有効になります。

DNS サーバの自動切り替え機能（逆引き）

ProxyDNS は、先に説明した順引きとは逆に、IP アドレスごとに使用したい DNS サーバを切り替えて中継できます。ここでは、逆引きの場合を例に説明します。



通信条件

- 会社の DNS サーバを使う場合
  使用するネットワークアドレス　：192.168.0.0
  DNS サーバの IP アドレス　：192.168.2.2
- インターネット上の DNS サーバを使う場合
  使用するネットワークアドレス　：192.168.0.0 以外
  DNS サーバの IP アドレス　：100.100.100.100

パソコン側の設定を確認する

1. **パソコン側が DHCP クライアントかどうか確認します。**

DHCP クライアントでない場合は設定します。

参照 ProxyDNS の設定をする→「Q&A　Q17 」（P.145 ）

こんな事に気をつけて

文字入力フィールドには半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「 ”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

5

詳細設定で ProxyDNS 情報を設定する

1. **詳細設定メニューで「ProxyDNS 情報」をクリックします。**

「ProxyDNS 情報」ページが表示されます。

2. **［逆引き情報一覧］で［追加］ボタンをクリックします。**

「ProxyDNS 情報設定（逆引き）」ページが表示されます。

3. **以下の項目を指定します。**

- IP アドレス　→ 192.168.0.0
- アドレスマスク　→ 24
- 動作　→設定した DNS サーバへ問い合わせる
- DNS サーバアドレス　→ 192.168.2.2

IPアドレス 192 . 168 . 0 . 0
アドレスマスク 24 (255.255.255.0)
動作
廃棄する
設定したDNSサーバへ問い合わせる
DNSサーバアドレス 192 . 168 . 2 . 2

4. **［更新］ボタンをクリックします。**

「ProxyDNS 情報」ページに戻ります。

5. **手順 2. ～ 4. の処理を繰り返し、以下の情報を設定します。**

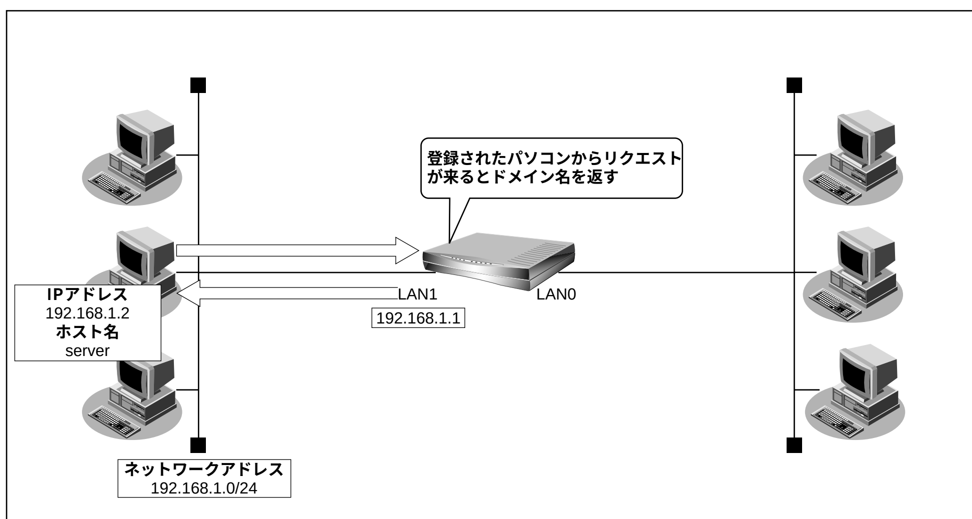
- IP アドレス　→なにも設定しない
- アドレスマスク　→ 0
- 動作　→設定した DNS サーバへ問い合わせる
- DNS サーバアドレス　→ 100.100.100.100

6. **［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

DNS サーバ機能

NetVehicle のホストデータベースにホスト名と IP アドレスのペアを登録しておきます。登録されたホストに対する DNS リクエストがあった場合は、ProxyDNS が DNS サーバの代わりに応答します。LAN 内の情報をあらかじめホストデータベースに登録しておくと、LAN 内のホストの DNS リクエストによって回線が接続されてしまうといったトラブルを防止できます。



通信条件

- 登録するホスト名　　：server
- 登録する IP アドレス　：192.168.1.2

パソコン側の設定を確認する

1. **パソコン側が DHCP クライアントかどうか確認します。**

DHCP クライアントでない場合は設定します。

参照 ProxyDNS の設定をする→「Q&A　Q17 」(P.145)

こんな事に気をつけて

文字入力フィールドには半角文字（0 〜 9、A 〜 Z、a 〜 z、および記号）だけを使用してください。ただし、空白文字、「 ”」、「<」、「>」、「&」、「%」 は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

詳細設定で DNS サーバ機能を設定する

1. 詳細設定メニューで「ホストデータベース情報」をクリックします。

「ホストデータベース情報」ページが表示されます。

2. 未設定の欄の［修正］ボタンをクリックします。

「ホストデータベース情報設定」ページが表示されます。

3. 以下の項目を指定します。

- ホスト名　　　　→ server
- IP アドレス　　　→ 192.168.1.2

補足 ホストデータベース情報は「リモートパワーオン機能」、「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。

4. ［更新］ボタンをクリックします。

「ホストデータベース情報」ページに戻ります。

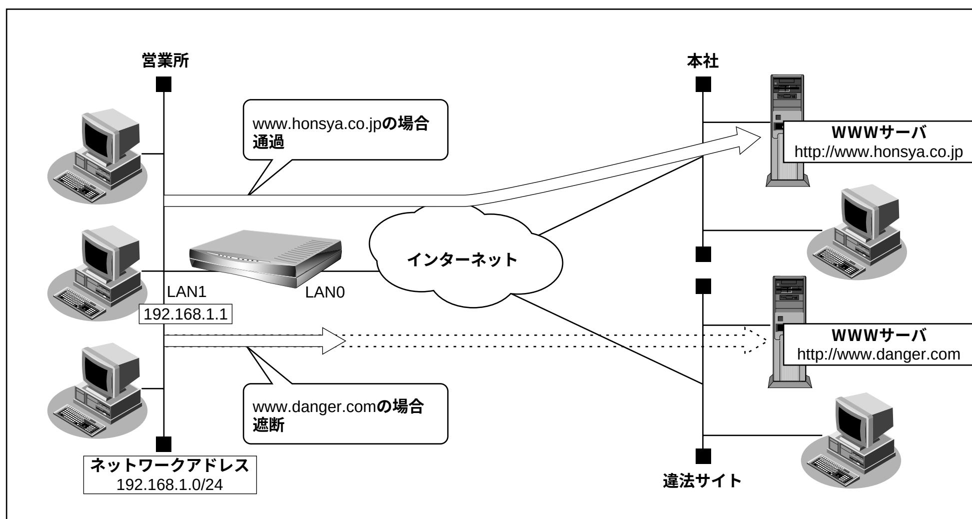
5. ［設定反映］ボタンをクリックします。

設定した内容が有効になります。



特定の URL へのアクセスを禁止する（URL フィルタ機能）

NetVehicleの「URLフィルタ機能」を利用すると、特定のURLへのアクセスを禁止することができます。
URL フィルタ機能を使用する場合は、「ProxyDNS 情報」で設定します。
以下に設定例を説明します。



通信条件

- **アクセスを禁止するドメイン名：www.danger.com**



こんな事に気をつけて

- URL フィルタ機能を使用する場合は、LAN 内のパソコンが NetVehicle の IP アドレスを DNS サーバの IP アドレスとして登録する必要があります。
- 文字入力フィールドには半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「 ”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

5

詳細設定でURLフィルタの情報を設定する

1. **詳細設定メニューで「URLフィルタ情報」をクリックします。**

「ProxyDNS情報」ページが表示されます。

2. **［順引き情報一覧］の［追加］ボタンをクリックします。**

「ProxyDNS情報設定（順引き）」ページが表示されます。

3. **以下の項目を指定します。**

- ドメイン名 →www.danger.com
- 動作 →廃棄する

ドメイン名	www. danger. com
動作	◉ 廃棄する ○ 設定したDNSサーバへ問い合わせる DNSサーバアドレス [ ].[ ].[ ].[ ]

4. **［更新］ボタンをクリックします。**

「ProxyDNS情報」ページに戻ります。

5. **［設定反映］ボタンをクリックします。**

設定した内容が有効になります。



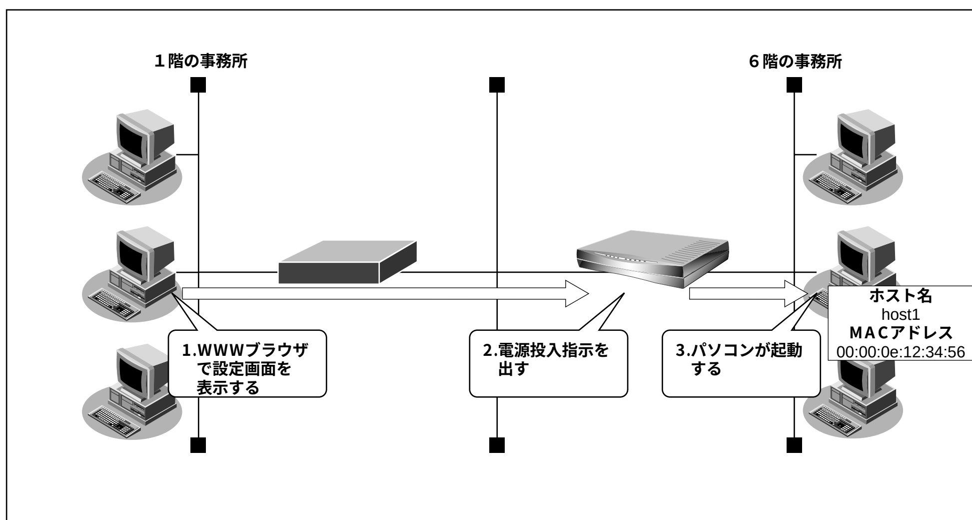
◆「＊」は使えるの？

例えば「www.danger.com」と「XXX.danger.com」の両方をURLフィルタの対象とする場合は「＊.danger.com」と指定することで両方を対象にできます。



遠隔地のパソコンを起動させる（リモートパワーオン機能）

リモートパワーオン機能は、NetVehicle につながっている離れた所にあるパソコンを、WWW ブラウザから Wakeup on LAN 機能を使用して起動させることができます。
ここでは、1 階の事務所のパソコンから 6 階の事務所のパソコンを起動する場合を例に説明します。



通信条件
［本社側］
- 起動するパソコンのホスト名　：host1
- 起動するパソコンの MAC アドレス　：00:00:0e:12:34:56



◆ Wakeup on LAN 機能とは？

AMD 社が開発したネットワーク上の電源 OFF 状態のパソコンを遠隔操作で起動する機能です。起動は Magic Packet と呼ばれるパケットを送付して行います。なお、Wakeup on LAN 機能はパソコンを起動するだけで電源 OFF は行いません。
電源 OFF する場合は、別途、電源制御用ソフトウェアが必要になります。

・本機能は、Wakeup on LAN に対応したパソコンだけで利用できます。Wakeup on LAN 対応機種については、パソコンのメーカーにお問い合わせください。

・本機能は、WWW ブラウザで NetVehicle のトップページが表示できる環境で利用できます。

詳細設定でリモートパワーオン情報を設定する

1. 詳細設定メニューで「ホストデータベース情報」をクリックします。

「ホストデータベース情報」ページが表示されます。

2. 未設定の欄の［修正］ボタンをクリックします。

「ホストデータベース情報設定」ページが表示されます。

3. 以下の項目を指定します。

- ホスト名　→host1
- MAC アドレス　→00:00:0e:12:34:56
- リモート電源制御　→対象

補足
・ホストデータベース情報は「リモートパワーオン機能」、「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。
・ホスト名は必須の設定項目ではありませんが、実際にリモートパワーオンを実行する場合にホスト情報一覧から目標とするパソコンを選択するのに有効な情報になります。



MAC アドレスの調べかた→「IP アドレスなどの設定を確認する」（P. 35）

ホスト名	host1
IPアドレス	. . .
MACアドレス	00 : 00 : 0e : 12 : 34 : 56
リモート電源制御	◉ 対象 ○ 対象外

4. ［更新］ボタンをクリックします。

「ホストデータベース情報」ページに戻ります。

5. ［設定反映］ボタンをクリックします。

設定した内容が有効になります。

リモートパワーオン機能を使う

1. パソコン上の WWW ブラウザで、起動させたいパソコンがつながっている NetVehicle のトップページを表示します。

2. 操作メニューで「リモートパワーオン」をクリックします。

「リモートパワーオン」ページが表示されます。

3. 起動させたいパソコンの［オン］ボタンをクリックします。

NetVehicle が該当するパソコンに対して「Magic Packet」を送信し、パソコンが起動します。

補足　パソコンがMagic Packetを受信してから起動が完了するまで、数十秒から数分かかります（お使いの機種やOSによって異なります）。



スケジュール機能を使う

NetVehicleのスケジュール機能では、リモートパワーオンを行う時間を登録できます。スケジュール予約情報を登録しておくと、毎日決まった時間にパソコンを起動するといった作業をNetVehicleが自動的に行います。ここでは、毎朝 8 時に特定のパソコンを起動する場合を例に説明します。



こんな事に気をつけて

- 設定前に NetVehicle の内部時計を正しくセットしてください。
- 本機能は、Wakeup on LAN に対応したパソコンだけ利用できます。Wakeup on LAN 対応機種については、パソコンのメーカーにお問い合わせください。
- 本機能を利用するには、あらかじめ利用するパソコンを「ホストデータベース情報設定」－「リモート電源制御」を「対象」として登録しておく必要があります。また、スケジュール機能を使ってリモートパワーオンする場合、「リモート電源制御」が「対象」となっているすべてのパソコンが起動します。

5

リモートパワーオンを予約する

1.　詳細設定メニューで「スケジュール情報」をクリックします。

「スケジュール情報」ページが表示されます。

[月間／週間予約一覧]

＼	動作	予約時刻	周期	修正／削除
1	-	-	-	修正　削除
2	-	-	-	修正　削除
3	-	-	-	修正　削除

2.　[月間 / 週間予約一覧] で未設定の欄の [修正] ボタンをクリックします。

「月間 / 週間予約設定」ページが表示されます。

3.　以下の項目を設定します。

- 予約時刻　→ 08:00/ 毎日

動作	リモートパワーオン	
予約時刻	08 : 00	◉ 毎日 ○ 毎週 ☐ 日曜日 ☐ 月曜日 ☐ 火曜日 ☐ 水曜日 ☐ 木曜日 ☐ 金曜日 ☐ 土曜日 ○ 毎月 ［　］ 日

4.　[更新] ボタンをクリックします。

「スケジュール情報」ページに戻ります。

5.　[設定反映] ボタンをクリックします。

設定した内容が有効になります。



SNMP エージェント機能を使う

NetVehicleは、SNMP(Simple Network Management Protocol)エージェント機能を利用できます。ここでは、NetVehicle が SNMP マネージャに対して MIB 情報を通知する例を説明します。

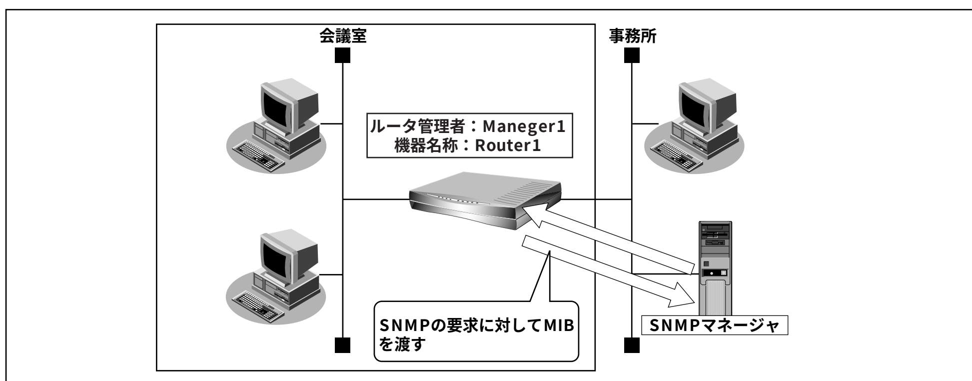


◆ SNMP とは？

SNMP(Simple Network Management Protocol)は、ネットワーク管理用のプロトコルです。SNMPマネージャは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMPエージェントはマネージャの要求に対して MIB(Management Information Base)という管理情報を返します。また、特定の情報については trap という機能を用いて、エージェントからマネージャに対して非同期通知を行うことができます。エージェントは、エージェントが起動されたとき、またはマネージャから不正な要求を受けたときに trap を送信します。



MIB 一覧（P.153）



通新条件

- ルータ管理者　：Maneger1
- 機器名称　：Router1
- 機器設置場所　：Kaigishitsu1

SNMP 情報を設定する

1. **詳細設定メニューで「装置情報」をクリックします。**

「装置情報設定」ページが表示されます。

2. **[SNMP 情報] で以下の項目を指定します。**

- SNMP エージェント機能 →使用する
- ルータ管理者 → Manager1
- 機器名称指定 →指定する
- 機器名称 → Router1
- 機器設置場所 → Kaigishitsu1
- SNMP ホスト１ → public とする
- SNMP ホスト２ →指定しない

[SNMP情報]

SNMPエージェント機能	○ 使用しない ◉ 使用する
ルータ管理者	Manager1
機器名称指定	○ ルータ名称を使用する ◉ 指定する 機器名称 Router1
機器設置場所	kaigishitsu1
SNMPホスト1	◉ publicとする（任意のホストを対象とする） ○ 指定する コミュニティ名 IPアドレス . . . トラップ ◉ 送信しない ○ 送信する
SNMPホスト2	◉ 指定しない ○ 指定する コミュニティ名 IPアドレス . . . トラップ ◉ 送信しない ○ 送信する

3. **[更新] ボタンをクリックします。**

4. **[設定反映] ボタンをクリックします。**

設定した内容が有効になります。

5



VPN 機能を使う

VPN（Virtual Private Network）機能は、インターネットを経由して遠隔地の LAN をつなぎ、遠隔地の LAN 上のアプリケーションやデータをあたかも同じオフィスにある LAN のように利用できます。また、認証情報や、暗号情報を設定することにより、遠隔地間を流れるデータのセキュリティを確保できます。



こんな事に気をつけて

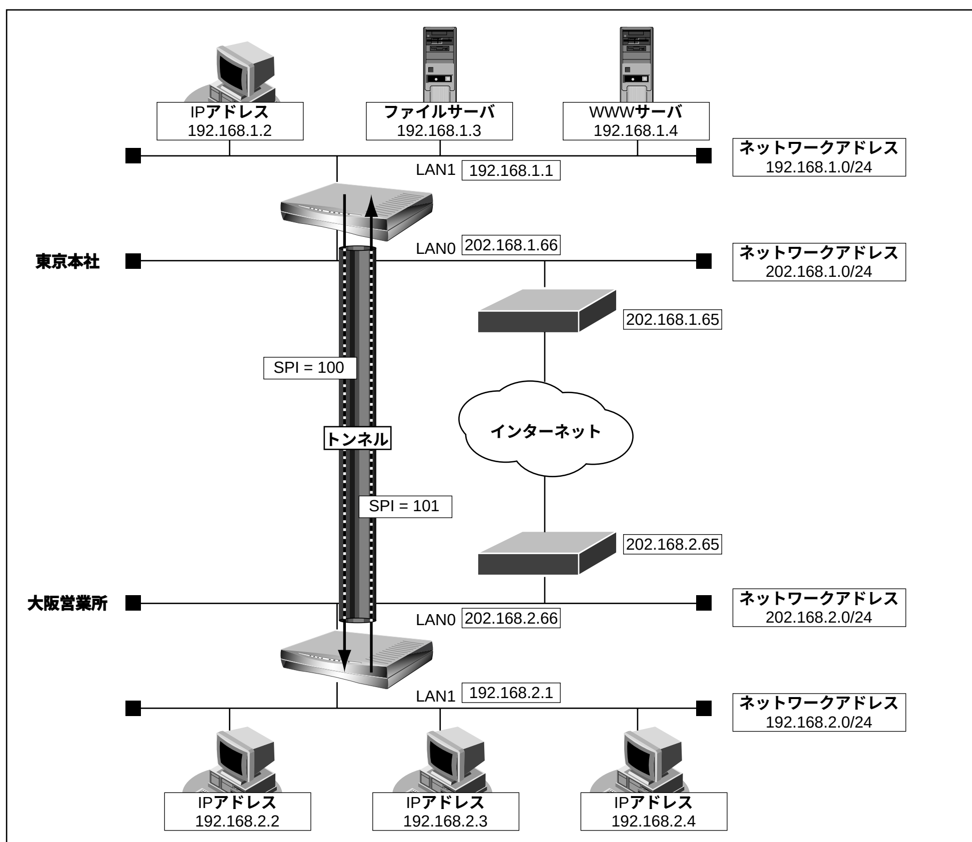
- VPN を構築する場合、相手ゲートウェイは NetVehicle である必要があります。
- VPN機能とダイナミックルーティングを併用するとダイナミックルーティングが有効にならない場合があります。スタティックルーティングで経路情報を指定してください。
- VPN 機能と NAT 機能は併用できません。併用する場合は、マルチ NAT（静的 NAT）を定義してください。



VPN とは？

暗号化技術や認証技術を使って、インターネットを仮想的な専用線として利用する技術です。また、VPN を使ってつないだルータ間の通信経路のことをトンネルと呼びます。

ここでは、以下の場合を例に説明します。



通信条件

- 東京本社から大阪営業所間の VPN 情報
  SPI　　　　　　　　　　　　：100
  認証アルゴリズムと認証秘密鍵　：hmac-md5、0101010101
  暗号アルゴリズムと暗号秘密鍵　：独自方式、0202020202
- 大阪営業所から東京本社間の VPN 情報
  SPI　　　　　　　　　　　　：101
  認証アルゴリズムと認証秘密鍵　：hmac-md5、0303030303
  暗号アルゴリズムと暗号秘密鍵　：独自方式、0404040404

[東京本社側]

- LAN0 側
- IP アドレス　：202.168.1.66
- ネットワークアドレス / ネットマスク　：202.168.1.0/24
- マルチ NAT を使用する

- LAN1 側
- IP アドレス　：192.168.1.1
- ネットワークアドレス / ネットマスク　：192.168.1.0/24

[大阪営業所側]

- LAN0 側
- IP アドレス　：202.168.2.66
- ネットワークアドレス / ネットマスク　：201.168.2.0/24
- マルチ NAT を使用する

- LAN1 側
- IP アドレス　：192.168.2.1
- ネットワークアドレス / ネットマスク　：192.168.2.0/24



◆ SPI とは？

トンネルの識別子です。SPI はトンネルの往路と復路でそれぞれ異なる値を定義します。トンネルをつなぐ NetVehicle を設定するときには、同じ方向のトンネルには同じ SPI を定義します。



こんな事に気をつけて

文字入力フィールドには半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「”」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。

東京本社側の NetVehicle を設定する

東京本社側で往路（東京本社→大阪営業所）の VPN 情報を設定する

1. **詳細設定メニューで「VPN 情報」をクリックします。**

「VPN 情報」ページが表示されます。

2. **[追加] ボタンをクリックします。**

「VPN 情報設定」ページが表示されます。

5

3. 以下の項目を指定します。

- SPI → 100
- 送信元情報（IP アドレス） → 192.168.1.0
- 送信元情報（アドレスマスク） → 24
- 宛先情報（IP アドレス） → 192.168.2.0
- 宛先情報（アドレスマスク） → 24
- ゲートウェイ IP アドレス → 202.168.2.66
- 認証情報（アルゴリズム） → hmac-md5
- 認証情報（秘密鍵） → 0101010101
- 暗号情報（アルゴリズム） →独自方式
- 暗号情報（秘密鍵） → 0202020202

SPI		100 （16進数）
送信元情報	IPアドレス	192 . 168 . 1 . 0
	アドレスマスク	24 (255.255.255.0)
宛先情報	IPアドレス	192 . 168 . 2 . 0
	アドレスマスク	24 (255.255.255.0)
ゲートウェイIPアドレス		202 . 168 . 2 . 66
認証情報	アルゴリズム	hmac-md5
	秘密鍵	0101010101 （16進数）
暗号情報	アルゴリズム	独自方式
	秘密鍵	0202020202 （16進数）

4. ［更新］ボタンをクリックします。

［VPN 情報］ページに戻ります。

東京本社側で復路（大阪営業所→東京本社）の VPN 情報を設定する

5. 手順 2. 〜 4. の処理を繰り返し、以下の情報を設定します。

- SPI → 101
- 送信元情報（IP アドレス） → 192.168.2.0
- 送信元情報（アドレスマスク） → 24
- 宛先情報（IP アドレス） → 192.168.1.0
- 宛先情報（アドレスマスク） → 24
- ゲートウェイ IP アドレス → 202.168.1.66
- 認証情報（アルゴリズム） → hmac-md5
- 認証情報（秘密鍵） → 0303030303
- 暗号情報（アルゴリズム） →独自方式
- 暗号情報（秘密鍵） → 0404040404

6. ［更新］ボタンをクリックします。

7. **詳細設定メニューで「LAN0 情報」をクリックします。**

「LAN0 情報設定」ページが表示されます。

8. **［静的 NAT 情報一覧］で［追加］ボタンをクリックします。**

「静的 NAT 情報設定」ページが表示されます。



こんな事に気をつけて

動的 NAT と静的 NAT が混在する場合、動的 NAT で使用する IP アドレスと静的 NAT で使用する IP アドレスは重複しないようにしてください。

9. **以下の情報を設定します。**

- プライベート IP 情報（IP アドレス）　→ 202.168.2.66
- プライベート IP 情報（ポート番号）　→すべて
- グローバル IP 情報（IP アドレス）　→ 202.168.2.66
- グローバル IP 情報（ポート番号）　→すべて
- プロトコル　→ esp

プライベートIP情報	IPアドレス	202 . 168 . 2 . 66
	ポート番号	すべて (番号指定:) "その他"を選択時のみ有効です)
グローバルIP情報	IPアドレス	202 . 168 . 2 . 66
	ポート番号	すべて (番号指定:) "その他"を選択時のみ有効です)
プロトコル		esp (番号指定:) "その他"を選択時のみ有効です)



◆ VPN で使用するプロトコル

VPNで使用するプロトコルは、認証情報と暗号情報の組み合わせにより決まります。認証情報を定義し、暗号情報を定義しない場合のプロトコルは、「ah」を指定します。それ以外の場合のプロトコルは、「esp」を指定します。

10. **［更新］ボタンをクリックします。**

「LAN0 情報設定」ページに戻ります。

11. **［更新］ボタンをクリックします。**

12. **［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

大阪営業所側の NetVehicle を設定する

「東京本社の NetVehicle を設定する」を参考に、大阪営業所の NetVehicle を設定します。その際、特に指定がないものは、東京本社と同じ設定にします。

大阪営業所側で往路（大阪営業所→東京本社）の VPN 情報を設定する

「VPN 情報設定」

- SPI → 101
- 送信元情報（IP アドレス） → 192.168.2.0
- 送信元情報（アドレスマスク） → 24
- 宛先情報（IP アドレス） → 192.168.1.0
- 宛先情報（アドレスマスク） → 24
- ゲートウェイ IP アドレス → 202.168.1.66
- 認証情報（アルゴリズム） → hmac-md5
- 認証情報（秘密鍵） → 0303030303
- 暗号情報（アルゴリズム） →独自方式
- 暗号情報（秘密鍵） → 0404040404

大阪営業所側で復路（東京本社→大阪営業所）の VPN 情報を設定する

「VPN 情報設定」

- SPI → 100
- 送信元情報（IP アドレス） → 192.168.1.0
- 送信元情報（アドレスマスク） → 24
- 宛先情報（IP アドレス） → 192.168.2.0
- 宛先情報（アドレスマスク） → 24
- ゲートウェイ IP アドレス → 202.168.2.66
- 認証情報（アルゴリズム） → hmac-md5
- 認証情報（秘密鍵） → 0101010101
- 暗号情報（アルゴリズム） →独自方式
- 暗号情報（秘密鍵） → 0202020202

VPN とマルチ NAT を併用するために静的 NAT を設定する

「静的 NAT 情報設定」

- プライベート IP 情報（IP アドレス） → 202.168.1.66
- プライベート IP 情報（ポート番号） →すべて
- グローバル IP 情報（IP アドレス） → 202.168.1.66
- グローバル IP 情報（ポート番号） →すべて
- プロトコル → esp

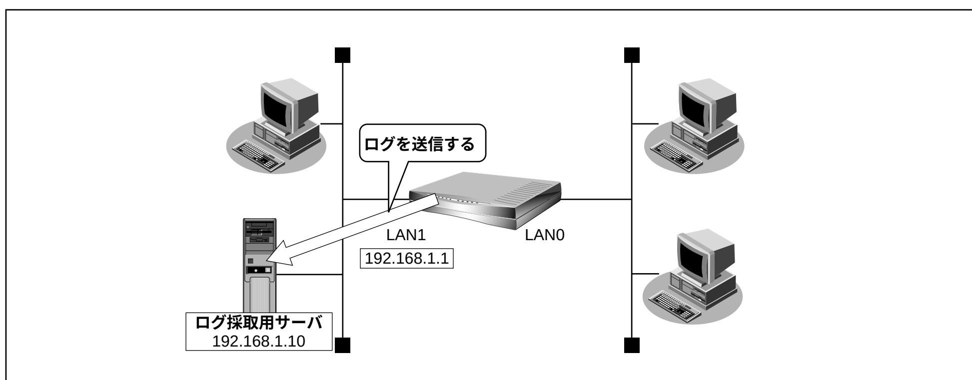


セキュリティログを採取する

NetVehicle のセキュリティログは、表示メニューで確認することができます。そのためには、あらかじめ採取するログを設定しておく必要があります。
NetVehicle で採取可能なセキュリティログは以下のとおりです。

- IP フィルタ
- URL フィルタ
- NAT
- DHCP

ここでは、採取したログをサーバに送信する場合を例に説明します。



通信条件

- 採取するログ　　　　　　　　：IP フィルタ、NAT
- ログ受信用サーバの IP アドレス　：192.168.1.10

採取するセキュリティログを選択する

1. 詳細設定メニューで「装置情報」をクリックします。

「装置情報設定」ページが表示されます。

2. [システムログ情報] で以下の項目を指定します。

- セキュリティログ　→ IP フィルタ、NAT
- システムログ送信　→送信する
- 送信先ホスト　　　→ 192.168.1.10

[システムログ情報]

セキュリティログ	☑ IPフィルタ ☐ URLフィルタ ☑ NAT ☐ DHCP
システムログ送信	○ 送信しない ◉ 送信する 送信先ホスト 192 . 168 . 1 . 10

3. **［更新］ボタンをクリックします。**

4. **［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

採取したセキュリティログを確認する

採取したセキュリティログの確認のしかたは、お使いのサーバによって異なります。ここでは、NetVehicle で確認する方法を説明します。

1. **表示メニューで「システムログ」をクリックします。**

［システムログ］が表示されます。

【システムログ】

```
Jan 01 09:00:08 init: system startup now.
Jan 01 15:22:58 enabled: system configuration restarted
Jan 01 15:23:55 protocol: NAT:table: UDP 192.168.1.3 -> 10.234.77.20:53
Jan 01 15:23:55 protocol: NAT:table: UDP 10.232.79.224 -> 10.232.16.12:53
Jan 01 15:23:55 protocol: NAT:table: TCP 192.168.1.3 -> 10.232.77.22:21
Jan 01 15:24:12 protocol: NAT:table: TCP 192.168.1.3 -> 10.232.77.22:20
Jan 01 15:42:36 protocol: NAT:table: TCP 192.168.1.3 -> 10.234.21.61:23
```



運用管理とメンテナンス

この章では、
NetVehicle の運用管理や確認の方法を説明します。



メンテナンス機能を使う

NetVehicle には、ファームウェア更新や、構成定義情報の設定や退避／復元などのメンテナンス方法として以下の 2 つの方法があります。

- WWW ブラウザによるメンテナンス
- FTP サーバ機能によるメンテナンス

WWW ブラウザによるメンテナンス

NetVehicle は WWW ブラウザを使用して、以下のメンテナンスが行えます。

●構成定義情報の退避／復元

現在の NetVehicle の構成定義情報を WWW ブラウザ機能により、退避／復元することができます。



「構成定義情報を退避する／復元する」（P.117 ）

●ファームウェア更新

WWW ブラウザを使用して FTP サーバ上の最新ファームウェアに更新することができます。
インターネットに接続している場合は、NetVehicle のサポートページから最新ファームウェアをダウンロードすることができます。
インターネットに接続していない場合は、ネットワーク上の FTP サーバに最新ファームウェアを置き、そこからダウンロードさせます。



「NetVehicle のファームウェアを更新する」（P.116 ）

FTP サーバ機能によるメンテナンス

NetVehicle は FTP サーバ機能を持っており、パソコンや UNIX システムの FTP コマンドを使ってメンテナンスができます。このため、インターネットにアクセスできない場合や、ネットワーク上に FTP サーバが存在しない場合でもメンテナンスができます。
また、スクリプトを作成することにより、複数の NetVehicle に対してこれらの作業を一括して行えます。
本機能により、以下のメンテナンスが行えます。

●構成定義情報の退避／復元

FTP コマンドの get/put により構成定義情報の退避／復元ができます。

●ファームウェア更新

あらかじめパソコン上に置いた最新ファームウェアを FTP コマンドによって更新できます。



◆ **FTP サーバ機能**

TCP/IP のファイル転送プロトコルである FTP によるファイル転送サービスを提供する機能のことです。NetVehicle の FTP サーバ機能は、構成定義情報の退避／更新およびファームウェア更新だけができます。



「FTP サーバ機能を使ってメンテナンスする」（P.118 ）



操作メニューを使う

操作メニューでは、回線の疎通が確認できます。また、時刻の設定方法、リモートパワーオンを管理できます。

操作メニューを表示する

1. **NetVehicle のトップページで、画面上部の［操作］アイコンをクリックします。**
操作メニューが表示されます。

ネットワークの接続を確認する

ping コマンドを使って、IP 接続が成立しているかどうか確認できます。

1. **操作メニューで「疎通確認」をクリックします。**
「疎通確認（ping)」ページが表示されます。

疎通確認(ping)

このページでは、pingコマンド(ICMP ECHOパケット)による通信の確認ができます。

ping送信先	

設定終了後、ping送信をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

[Ping送信] [キャンセル]

2. **「ping 送信先」に送信先の IP アドレスを入力します。**

3. **［ping 送信］ボタンをクリックします。**
「ping 実行中」というメッセージが表示されたあと、ping 送信結果が表示されます。

6

時刻を設定する

NetVehicle の内部時計の時刻を設定できます。時刻設定するには以下の３通りの方法があります。

- WWW ブラウザを利用しているパソコンの時刻を設定する方法
- ネットワーク上の TIME サーバまたは NTP サーバから時刻を取得する方法
- 任意の時刻を設定する方法

ここでは任意の時刻を設定する場合を例に説明します。

1. **操作メニューで「時刻設定」をクリックします。**

「時刻情報設定」ページが表示されます。

時刻情報設定

電源を切断しますと時刻は初期化されます。

[時刻の設定]

パソコンから時刻を取得	パソコンの現在時刻 2002 年 3 月 15 日 10 時 33 分 18 秒	設定
タイムサーバから時刻を取得	サーバアドレス DHCPで自動設定されています	設定
任意の時刻を設定	1970 年 01 月 01 日 00 時 00 分 00 秒	設定

2. **「任意の時刻を設定」を指定する場合は現在の日時を入力します。**
指定する時刻の設定方法の［設定］ボタンをクリックします。

「時刻を○○○○に設定しました。」というメッセージが表示されます。

こんな事に気をつけて

電源を切ると設定した内容は無効になります。



表示メニューを使う

表示メニューでは、DHCP 情報、NAT 情報、ルーティング情報、IP 統計情報、LAN 情報、VPN 情報、システムログ、現在時刻、および経過時間情報を確認できます。

表示メニューを表示する

1. **NetVehicle のトップページで、画面上部の［表示］アイコンをクリックします。**
表示メニューが表示されます。

表示メニューで確認できる情報

以下の情報が確認できます。

「DHCP 情報」
使用している IP アドレス等の情報を確認できます。

「NAT 情報」
NAT のセッションの状態を確認できます。

「ルーティング情報」
ルーティングテーブルを確認できます。

「IP 統計情報」
ルーティングした通信のプロトコルごとの内訳を確認できます。

「LAN 情報」
LAN の統計情報を確認できます。

「VPN 情報」
VPN 情報を確認できます。

「システムログ」
システム運用状況の履歴が確認できます。

「現在時刻」
現在時刻を確認できます。

「経過時間情報」
電源投入後、経過した時間を確認できます。



メンテナンスメニューを使う

メンテナンスメニューでは、バージョン情報、エラーログ情報、構成定義情報の確認、およびファームウェアの更新ができます。

メンテナンスメニューを表示する

1. **NetVehicle のトップページで、画面上部の［メンテナンス］アイコンをクリックします。**
メンテナンスメニューが表示されます。

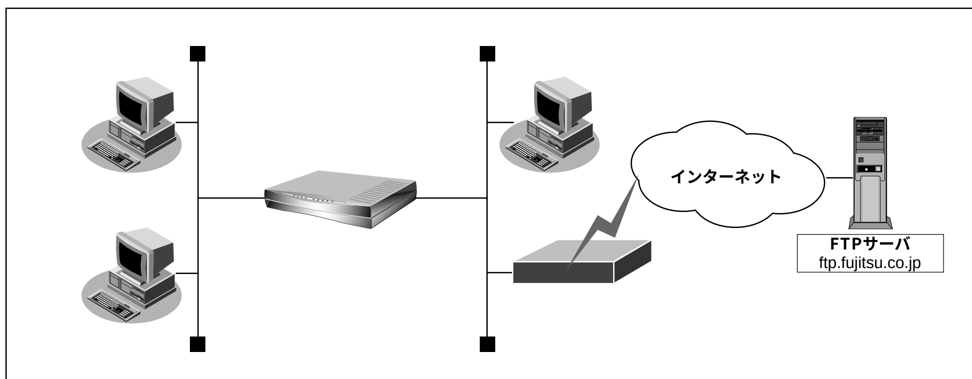
NetVehicle のファームウェアを更新する

ファームウェアを更新すると、NetVehicle に新しい機能を追加できます。

 **こんな事に気をつけて**

- ファームウェアの更新中は、NetVehicle の電源を切らないでください。
- ファームウェアを更新する前に、構成定義情報を退避しておいてください。

 構成定義情報を退避する / 復元する（P.117）



1. **メンテナンスメニューで「ファームウェア更新」をクリックします。**

以下の情報をもとにファームウェアを更新します。情報に誤りがない場合はOKボタンをクリックしてください。

[注意]ファームウェアの更新中は電源を切らないでください。以後、正常に動作しなくなる可能性があります。

転送元ホストIPアドレス	ログインID	ログインパスワード	ファイルロケーション
ftp.fujitsu.co.jp	ftp	hamster@fujitsu.co.jp	/pub/NV/firm/L10SOFT.ftp

OK

2. **表示されている内容を確認し、正しければ［OK］ボタンをクリックします。**
ファームウェアの更新が始まります。

3. **ファームウェア更新の終了を通知するポップアップ画面が表示されたら、［OK］ボタンをクリックします。**
NetVehicle が再起動し、更新したファームウェアが有効になります。

4. ［トップページに戻る］ボタンをクリックします。

トップメニューに戻ります。


・インターネットに接続していないネットワークでファームウエアを更新する場合、更新するファームウェアをネットワーク内の FTP サーバに配置してください。最新のファームウェアは、NetVehicle のサポートページで公開しています。

・ファームウェアを更新するための情報を「詳細設定」の「装置情報」にあるファームウェア更新情報に設定して 1. 〜 4. の操作を行ってください。設定情報は、以下の４項目です。

- 転送元 IP アドレス（FTP サーバの IP アドレス）
- ログイン ID
- ログインパスワード
- ファイルロケーション（ファームウェアを配置した場所）

ファームウェア更新に失敗した場合には、バックアップファームを起動すると正常に起動が行えます。


「ファームウェア更新に失敗したときには（バックアップファーム機能）」（P.129 ）

構成定義情報を退避する／復元する

現在の NetVehicle の構成定義情報をファイルに保存し、退避しておきます。必要になったときに保存しておいた構成定義情報を復元できます。

- **構成定義情報の退避：　メンテナンスメニューの「構成定義情報」ページを、WWW ブラウザ機能を使ってファイルに保存します。**
- **構成定義情報の復元：　WWW ブラウザで保存しておいた「構成定義情報」ページのファイルを開き、［復元］ボタンをクリックします。**

6


こんな事に気をつけて

現在の NetVehicle の IP アドレスと保存時の IP アドレスが異なると復元できません。

メンテナンスメニューで確認できる情報

上記で説明した情報以外に以下の情報が確認できます。

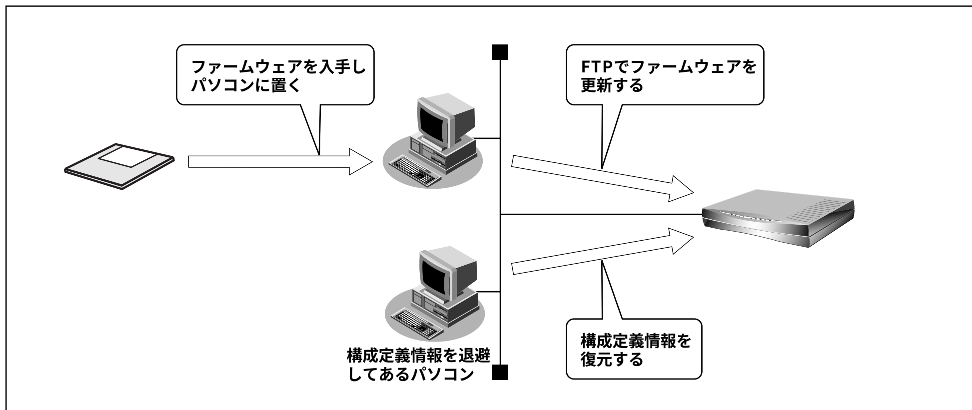
「バージョン情報」
現在のファームウェアのバージョンを確認できます。

「エラーログ情報」
NetVehicle 本体の異常に関する情報が記録されている場合は、ここで確認できます。



FTP サーバ機能を使ってメンテナンスする

NetVehicleはFTPサーバ機能を持っており、パソコンやUNIXシステムのftpコマンドを使って構成定義情報の退避／復元およびファームウェア更新ができます。



FTP サーバ機能を利用するときのユーザ名、パスワードは以下のとおりです。

- ユーザ名　　：ftp-admin
- パスワード　：詳細設定で設定した管理者パスワードを指定します。

 管理者パスワードを設定していない場合は、FTP サーバ機能もパスワードがないものとして動作します。

●メンテナンス対象のファイル

FTP サーバ機能でメンテナンス対象となるファイル名は以下のとおりです。

- 構成定義情報　　：config
- ファームウェア　：firmware

●再起動方法

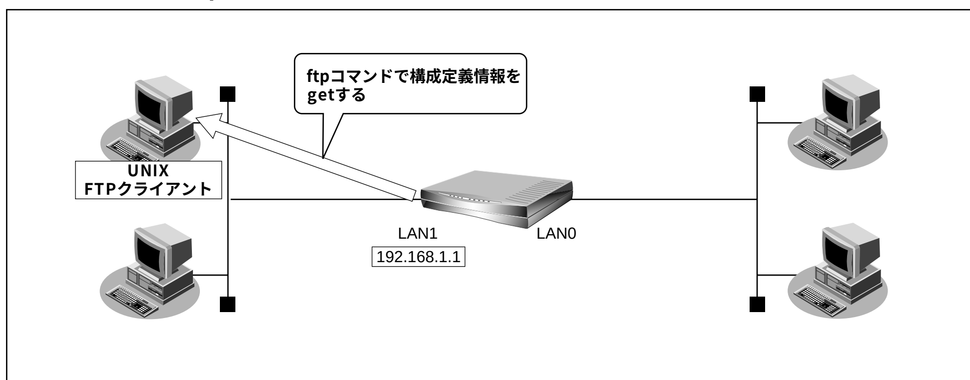
ftp コマンドのサブコマンドとして「get reset」を入力すると NetVehicle を再起動します。

こんな事に気をつけて

セキュリティ確保のため管理者パスワードを設定することを強く推奨します。
設定しない場合、ネットワーク上の誰からでもアクセスできるため非常に危険です。

FTP サーバ機能による構成定義情報の退避

UNIX システムの ftp コマンドを使って構成定義情報を退避する場合について説明します。



 **こんな事に気をつけて**

メンテナンス作業時は、必ず以下のことを守ってください。

- NetVehicle の電源を切らないでください。
- NetVehicle 上でデータ通信していないことを確認してください。
- WWW ブラウザ、コンソールによる設定作業を一切していない状態で行ってください。

● ftp コマンドの使用例

構成定義情報（config）を UNIX システム上の config1 ファイルに退避する場合の例を示します。

```
# cd 構成定義情報格納ディレクトリ
# ftp 192.168.1.1                              ：NetVehicle に接続する

Connected to 192.168.1.1.
220 NetVehicle-L10 FTP server(Ver1.0) ready.
Name (192.168.1.1:root): ftp-admin             ：ユーザ名を入力する

331 Password required for ftp-admin.
Password:                                      ：パスワードを入力する

230 User ftp-admin logged in.
ftp> bin                                       ：バイナリモードにする

200 Type set to I.
ftp> get config config1                    ：構成定義情報(config)を config1 ファイルに格納する

local: config remote: config1
200 PORT command successful.
150 Opening BINARY mode data connection for 'config' (2753 bytes).
226 Transfer complete.
2857 bytes received in 1.10 seconds (2.44 Kbytes/s)
ftp> bye                                       ：処理を終了する

221 Goodbye.
#
```

 パスワードは、詳細設定の「パスワード情報」で設定した管理者パスワードを指定してください。

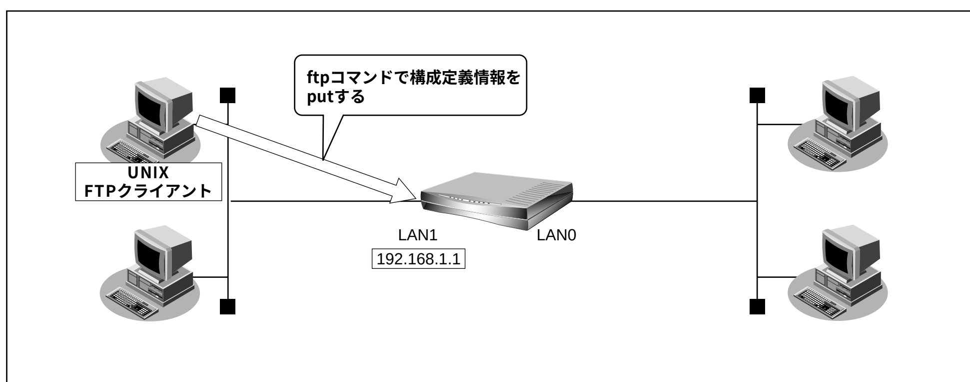
●スクリプト(B シェル)の例

IPアドレスとして192.168.1.1と192.168.2.1を持つNetVehicleの構成定義情報を退避する場合の例を示します。

```
#!/bin/sh
ftp -vn <<!EOF                # ftp コマンドを起動する
open 192.168.1.1              # NetVehicle(192.168.1.1)に接続する
user ftp-admin password       # ユーザ名、パスワードを入力する
bin                           # バイナリモードにする
get config config1            # 構成定義情報(config)を config1 ファイルに格納する
close                         # NetVehicle とのセションを切断する
open 192.168.2.1              # NetVehicle(192.168.2.1)に接続する
user ftp-admin password       # ユーザ名、パスワードを入力する
bin                           # バイナリモードにする
get config config2            # 構成定義情報(config)を config2 ファイルに格納する
close                         # NetVehicle とのセションを切断する
bye                           # ftp コマンドを終了する
!EOF
```

FTP サーバ機能による構成定義情報の復元

UNIX システムの FTP コマンドを使って構成定義情報を復元する場合について説明します。



こんな事に気をつけて

メンテナンス作業時は、必ず以下のことを守ってください。

- NetVehicle の電源を切らないでください。
- NetVehicle 上でデータ通信していないことを確認してください。
- WWW ブラウザ、コンソールによる設定作業を一切していない状態で行ってください。

●ftp コマンドの使用例

構成定義情報（config）を UNIX システム上の config1 ファイルから復元する場合の例を示します。

```
# cd 構成定義情報格納ディレクトリ
# ftp 192.168.1.1                                    ：NetVehicle に接続する
Connected to 192.168.1.1.
220 NetVehicle-L10 FTP server(Ver1.0) ready.
Name (192.168.1.1:root): ftp-admin                   ：ユーザ名を入力する
331 Password required for ftp-admin.
Password:                                            ：パスワードを入力する
230 User ftp-admin logged in.
ftp> bin                                             ：バイナリモードにする
200 Type set to I.
ftp> put config1 config             ：config1 ファイルを構成定義情報（config）として書き込む
local: config1 remote: config
200 PORT command successful.
150 Opening BINARY mode data connection for 'config'.
226- Transfer complete.
update: File information check now!
update: File information check ok.
        :
226 Write complete.
2856 bytes sent in 1.10 seconds (2.44 Kbytes/s)
ftp> get reset                                       ：NetVehicle を再起動する
local: reset remote: reset
200 PORT command successful.
421 reset Request OK. bye.
ftp> bye                                             ：処理を終了する
#
```


・パスワードは、詳細設定の「パスワード情報」で設定した管理者パスワードを指定してください。

・ftp コマンドのサブコマンドとして「get　reset」を入力すると NetVehicle を再起動します。

●スクリプト（B シェル）の例

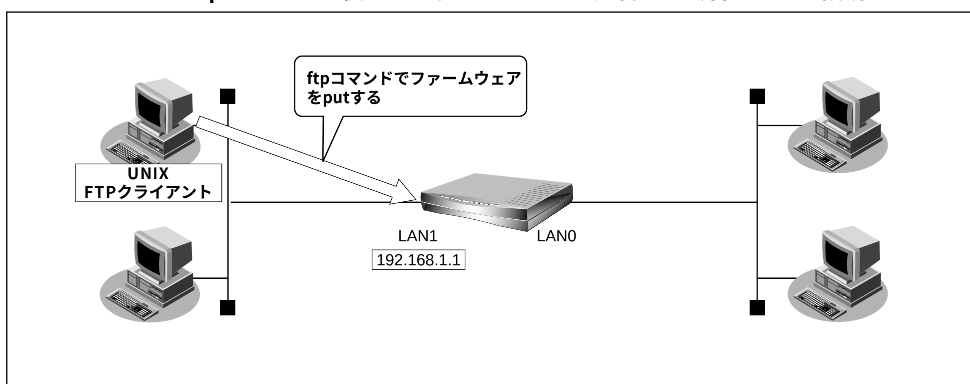
IP アドレスとして 192.168.1.1 と 192.168.2.1 を持つ NetVehicle の構成定義情報（config）を更新する場合の例を示します。

```
#!/bin/sh
ftp -vn <<!EOF               # ftp コマンドを起動する
open 192.168.1.1             # NetVehicle（192.168.1.1）に接続する
user ftp-admin password      # ユーザ名、パスワードを入力する
bin                          # バイナリモードにする
put config1 config           # config1 ファイルを構成定義情報（config）として書き込む
get reset                    # NetVehicle を再起動する
close                        # NetVehicle とのセションを切断する
open 192.168.2.1             # NetVehicle（192.168.2.1）に接続する
user ftp-admin password      # ユーザ名、パスワードを入力する
bin                          # バイナリモードにする
put config2 config           # config2 ファイルを構成定義情報（config）として書き込む
get reset                    # NetVehicle を再起動する
close                        # NetVehicle とのセションを切断する
bye                          # ftp コマンドを終了する
!EOF
```

6

FTP サーバ機能によるファームウェアの更新

UNIX システムの ftp コマンドを使ってファームウェアを更新する場合について説明します。



こんな事に気をつけて

メンテナンス作業時は、必ず以下のことを守ってください。

- NetVehicle の電源を切らないでください。
- NetVehicle 上でデータ通信していないことを確認してください。
- WWW ブラウザ、コンソールによる設定作業を一切していない状態で行ってください。
- ファームウェアを更新する前に、構成定義情報を退避しておいてください。

● ftp コマンドの使用例

ファームウェアを UNIX システム上から更新する場合の例を示します。

```
# cd 構成定義情報格納ディレクトリ
# ftp 192.168.1.1                                  ：NetVehicle に接続する
Connected to 192.168.1.1.
220 NetVehicle-L10 FTP server(Ver1.0) ready.
Name (192.168.1.1:root): ftp-admin                 ：ユーザ名を入力する
331 Password required for ftp-admin.
Password:                                          ：パスワードを入力する
230 User ftp-admin logged in.
ftp> bin                                           ：バイナリモードにする
200 Type set to I.
ftp> put L10SOFT.ftp firmware                      ：ファームウェアを書き込む
local: L10SOFT.ftp remote: firmware
200 PORT command successful.
150 Opening BINARY mode data connection for 'firmware'.
226- Transfer complete.
update: Transfer file check now!
update: Transfer file check ok.
          :
226 Write complete.
631966 bytes sent in 97.80 seconds (6.31 Kbytes/s)

ftp> get reset                                     ：NetVehicle を再起動する
local: reset remote: reset
200 PORT command successful.
421 reset Request OK. bye.
ftp> bye                                           ：処理を終了する

#
```


・パスワードは、詳細設定の「パスワード情報」で設定した管理者パスワードを指定してください。
・ftp コマンドのサブコマンドとして「get reset」を入力すると NetVehicle を再起動します。

●スクリプト（B シェル）の例

IP アドレスとして 192.168.1.1 と 192.168.2.1 を持つ NetVehicle のファームウェア（firmware）を更新する場合の例を示します。

```
#!/bin/sh
ftp -vn <<!EOF                  # ftp コマンドを起動する
open 192.168.1.1                # NetVehicle（192.168.1.1）に接続する
user ftp-admin password         # ユーザ名、パスワードを入力する
bin                             # バイナリモードにする
put L10SOFT.ftp firmware        # L10SOFT.ftp ファイルをファームウェア（firmware）としてを書き込む
get reset                       # NetVehicle を再起動する
close                           # NetVehicle とのセションを切断する
open 192.168.2.1                # NetVehicle（192.168.2.1）に接続する
user ftp-admin password         # ユーザ名、パスワードを入力する
bin                             # バイナリモードにする
put L10SOFT.ftp firmware        # L10SOFT.ftp ファイルをファームウェア（firmware）としてを書き込む
get reset                       # NetVehicle を再起動する
close                           # NetVehicle とのセションを切断する
bye                             # ftp コマンドを終了する
!EOF
```

6



困ったときには

この章では、
通信ができなくなった場合や、NetVehicle が故障した場合の
対処方法を説明します。



通信ができない場合には

通信ができない場合、さまざまな原因が考えられます。まず、以下を参考にNetVehicleの動作状況を確認してみてください。



◆エラーログ情報からトラブルの原因を探る

メンテナンスメニューの「エラーログ情報」ページに表示されたエラー番号から、エラーの原因をある程度特定できます。

エラーログ情報のページのプリントアウトを保管しておくことをお勧めします。

⚠警告

・決してご自身では修理を行わないでください。
・NetVehicleが故障した場合は、「NetVehicleサポートセンター」へ連絡の上、メンテナンスを受けてください。

起動時の動作に関するトラブル

NetVehicle起動時のトラブルには、以下のようなものがあります。

● POWERランプがつかない

【原因】電源ケーブルがコンセントに正しく接続されていない。

【対処】電源ケーブルをコンセントに正しく接続してください。

【原因】NetVehicleの電源スイッチが入っていない。

【対処】NetVehicleの電源スイッチが「｜」側に入っていることか確認してください。

●電源を入れてしばらくしてもCHECKランプが消灯しない

【原因】本体に以上が発生しました。

【対処】「NetVehicleサポートセンター」へ連絡してください。

NetVehicle設定時のトラブル

NetVehicle設定時のトラブルには、次のようなものがあります。

● WWWブラウザでマニュアルどおりのURLを指定したがNetVehicleのトップページが表示されない

【原因】接続に誤りがある。または、10BASE-Tケーブルが断線している。

【対処】接続したHUBポートに該当するHUB LEDが点灯しているかを確認してください。点灯していない場合には正しく接続されていないか、ケーブルが断線している可能性があります。パソコンとNetVehicleに10BASE-Tケーブルがきちんと差し込んであることを確認し、それでもHUB LEDが点灯しない場合には別の10BASE-Tケーブルに交換してみてください。

【原因】パソコンの IP アドレスやネットマスクが間違っている。

【対処】
- パソコンの設定でIPアドレスやネットマスクをしている場合には、NetVehicleと通信できるIPアドレスが設定されているかどうかを確認してください。NetVehicleのIPアドレスやネットマスクを変更していない場合には、パソコンには以下の範囲で設定を行う必要があります。
  IP アドレス　　　：192.168.1.2 ～ 192.168.1.254
  ネットマスク　　　：255.255.255.0
- NetVehicle の DHCP サーバ機能を利用している場合には、パソコンを再起動してください。
- Windows® 98 の場合は、「プライベート IP アドレス自動割り当て」機構により、DHCP サーバから自動取得する設定にしていても、169.254.XX.XX という IP アドレスが設定される場合があります。この場合は IP アドレスを固定で割り当てても通信できないことが多いため、ネットワークドライバと TCP/IP を入れ直してください。

補足 パソコン側の IP 設定は、winipcfg コマンド（Windows® 95/98/Me の場合）や ipconfig コマンド（WindowsNT®/Windows® 2000 の場合）で確認できます。

【原因】パソコンと TA でインターネットに接続したときの設定が残っている。

【対処】LAN インタフェースの IP アドレスを再割り当てするため、パソコンを再起動してください。

【原因】WWW ブラウザの設定が間違っている。

【対処】
・WWW ブラウザ（Microsoft Internet Explorer 5.5）の場合、[ツール] → [インターネットオプション] → [接続] において、インターネットオプション画面のダイヤルアップの設定で「ダイヤルしない」が選択されていることを確認してください。「通常の接続でダイヤルする」が選択されているとWWW ブラウザを起動するたびにモデムや TA からインターネットへ接続しようとして NetVehicle と通信できない可能性があります。
・WWW ブラウザの設定で Proxy サーバの設定が有効になっている可能性があります。[ツール] → [インターネットオプション] → [接続] → [LAN の設定] において、プロキシサーバの欄で「プロキシサーバを使用する」のチェックを外し、Proxy サーバを使用しない状態にしてください。また、Proxy サーバを使用する場合は、[プロキシの設定] において例外の欄に NetVehicle の IP アドレス（NetVehicle の IP アドレスを変更していない場合は 192.168.1.1）を追加してください。

【原因】パソコンの ARP エントリの値がおかしくなっている。

【対処】NetVehicle と同じ IP アドレスを持つ機器と通信した直後に、パソコンの電源を切らないまま NetVehicle へ接続変更を行った場合には通信できません。しばらく待つか、パソコンを再起動してください。

【原因】NetVehicle と同じ IP アドレスを持つ機器が接続されている。

【対処】IP アドレスが重複している機器が LAN 上に存在すると、正しく通信できません。NetVehicle から設定を行うパソコン以外を接続している 10BASE-T ケーブルを外し、パソコンを再起動してください。

【原因】NetVehicle の IP アドレスが変更されている。

【対処】変更後の NetVehicle の IP アドレスを指定してください。

【原因】パソコンの IP アドレスを変更していない。

【対処】NetVehicle の IP アドレスを変更した場合、必ずパソコン側の IP アドレスもそれに合わせて変更します。
① NetVehicle の DHCP サーバ機能を利用している場合：パソコンを再起動してください。
② NetVehicle の DHCP サーバ機能を利用していない場合：
パソコンの IP アドレスを NetVehicle と直接通信可能なアドレスに変更してください。また、ネットマスクを NetVehicle に設定した値と同じ値に設定してください。このとき、DNS サーバの IP アドレスも忘れずに入力してください。

●変更した NetVehicle の IP アドレスがわからなくなった
● NetVehicle に設定した管理者パスワードがわからなくなった

【対処】NetVehicle をご購入時の状態に戻してください。こうすることで管理者パスワードを削除し、IP アドレスを「192.168.1.1」に戻すことができます。それまでに設定した内容はすべて消えてしまいますので、最初から設定をやり直してください。



「ご購入時の状態に戻すには」（P.131）

データ通信に関するトラブル

NetVehicle でデータ通信を行う際のトラブルには、以下のようなものがあります。

●データ通信ができない

【原因】IP フィルタリング、ルーティング情報（NetVehicle/ 相手）または NAT の設定が間違っている。

【対処】
- IP フィルタリングの設定や NAT の設定をご利用のネットワーク環境や目的に合わせて、設定をやり直してみてください。
- 設定をやり直しても通信できない場合は、「NetVehicleサポートセンター」へ連絡してください。

【原因】LAN0 側の転送レートの自動認識に失敗した。

【対処】NetVehicleの100/10BASE-TX（LAN0ランプ、100Mランプ、FULLランプ）の状態とLAN0側に接続しているハブ装置の LINK 状態を確認します。両者の表示が異なっている場合は自動認識に失敗しています。NetVehicle の転送レートをハブ装置の仕様に合わせた転送レート（100Mbps- 全二重、100Mbps- 半二重、10Mbps- 半二重）に変更し、再接続してみてください。

● Ping の応答は正常だが、WWW ブラウザや電子メールは使えない

【原因】DNS の設定が間違っている。

【対処】本装置の DHCP サーバおよび ProxyDNS を使用するか、パソコン側で DNS サーバアドレスの設定を正しく行ってください。

●詳細設定で IP アドレスを変更し再起動したらまったくつながらなくなった

【原因】DHCP の設定が古い。

【対処】かんたん設定の場合、IP アドレス変更と連動して DHCP の割り当て先頭IP アドレスが書き変わりますが、詳細設定の場合、連動しないため、個別に設定を変更する必要があります。書き変えない場合、以下の状態になります。

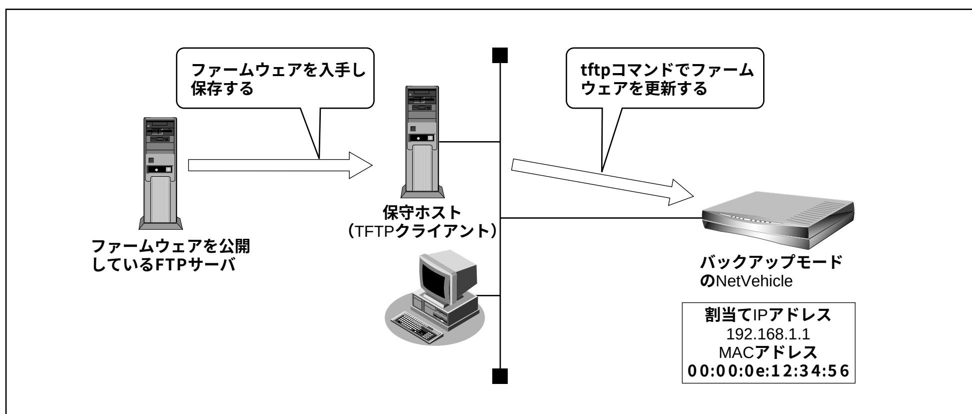
（例） NetVehicle の IP アドレスを「192.168.1.1」から「172.32.100.1」に変更した場合

	[変更前]		[変更後]	
	IP アドレス	DHCP 先頭 IP アドレス	IP アドレス	DHCP 先頭 IP アドレス
かんたん設定	192.168.1.1	192.168.1.2	172.32.100.1	172.32.100.2
細設定	192.168.1.1	192.168.1.2	172.32.100.1	192.168.1.2



ファームウェア更新に失敗したときには(バックアップファーム機能)

NetVehicle は停電などでファームウェアの更新に失敗し、起動できなくなった場合に、バックアップ用のファームを起動し、一時的に復旧することができます。なお、正常な状態に復旧するには、ネットワーク上の TFTP クライアントからファームウェアを転送する必要があります。



補足
・バックアップモードとは、バックアップ用のファームウェア（バックアップファーム）で起動している状態のことです。
・リセットスイッチを押しながら電源を入れるとバックアップファームが起動されます。

こんな事に気をつけて

システムによっては TFTP クライアント機能をサポートしていない場合があります。



◆ TFTP とは

UDP 上で動作するファイル転送サービスを行うためのプロトコルです。
FTP とは全く異なるプロトコルです。

以下にバックアップファームを使用してファームウェアを更新する手順を TFTP クライアントとして Sun OS5.4 を使った場合を例に説明します。

TFTP クライアントの準備をする

1. 更新するためのファームウェアを TFTP クライアントに保存します。

補足　NetVehicle の FTP サイトからダウンロードすることができます。

2. arp コマンドで NetVehicle の ARP エントリを登録します。

```
# arp -s 192.168.1.1 00:00:0e:12:34:56
```


NetVehicle の MAC アドレス→「底面のラベルについて」（P.134）

補足　バックアップモードで動作しているときは、自分あてにきたパケットの IP アドレスを自分の IP アドレスとして設定します。

NetVehicle の準備をする

1. **NetVehicle を TFTP クライアントが接続されているネットワークに接続します。**

2. **NetVehicle のリセットスイッチを押しながら電源を入れます。**

3. **CHECK、LAN0、100M、FULL、LAN1 ランプの緑点滅を確認し、リセットスイッチをはなすとバックアップモードで起動します。**

補足 バックアップモードで動作しているときは、CHECK ランプが緑色に点灯します。

ファームウェアを更新する

1. **TFTP クライアントの tftp コマンドを使って、NetVehicle にファームウェアを書き込みます。**

以下に、Sun OS5.4 から tftp コマンドを使ってファームウェアを更新する手順を記述します。

```
# cd ファームウェア格納ディレクトリ
# tftp
tftp> connect 192.168.1.1              ：NetVehicle に接続する
                                         ARP エントリで登録した IP アドレスを指定します
tftp> binary                           ：バイナリモードにする
tftp> put L10SOFT.ftp firmware         ：L10SOFT.ftp ファイルをファームウェア（firmware）として書き込む
tftp> quit                             ：処理を終了する
```

補足 バックアップモードで動作している時は、"firmware" というファイルを書き込むことでファームウェアの更新を行います。

こんな事に気をつけて

- ファームウェアの転送（put）中は、NetVehicle の電源を切らないでください。
- 転送中に電源を切ると、NetVehicle が使用できなくなる場合があります。

2. **ファームウェアの更新が正常に行われたことをランプで確認し、電源を切ります。**

補足 正常に更新が行われた場合、CHECK、LAN0、100M、FULL ランプが緑色に点滅します。

3. **電源を入れると、更新したファームウェアで NetVehicle が起動します。**



ご購入時の状態に戻すには

NetVehicleを誤って設定した場合やトラブルが発生した場合には、NetVehicleをご購入時の状態に戻すことができます。



こんな事に気をつけて

ご購入時の状態に戻すと、それまでの設定内容がすべて失われます。構成定義情報の退避、または設定内容をメモしておきましょう。



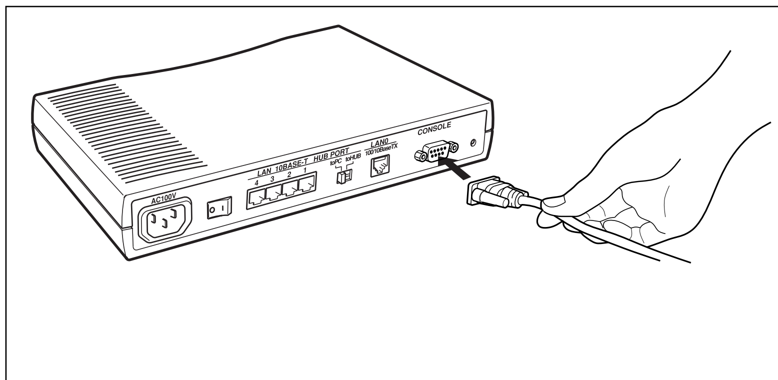
「構成定義情報を退避する／復元する」（P.117）

用意するもの

- RS232Cケーブル（クロス、NetVehicleに接続する側がメス型９ピンのD-SUBコネクタ）
- ターミナルソフト（Windows® 95/98やWindowsNT® 4.0に標準で装備されている「HyperTerminal」など）

NetVehicleとパソコンをRS232Cケーブルで接続する

1. NetVehicleとパソコンを接続します。



7

NetVehicle をご購入時の状態に戻す

1. **コンピュータでターミナルソフトを起動します。**

2. **通信条件を次のように設定します。**

スタート Bit	データ Bit	パリティ Bit	ストップ Bit	同期方式	通信速度	フロー制御
1	8	なし	1	非同期	9600	Xon/Xoff

補足 通信条件の設定方法については、ターミナルソフトのマニュアルを参照してください。

3. **[Return] キーまたは [Enter] キーを押します。**

4. **画面に「>」と表示されたことを確認します。**

補足 画面に「>」が表示されない場合は、通信条件の「フロー制御」を「なし」または「Xon/Xoff」にしてみてください。

5. **キーボードから logon と入力して、[Return] キーまたは [Enter] キーを押します。**

6. **画面に「#」と表示されたことを確認します。**

7. **キーボードから reset clear と入力して、[Return] キーまたは [Enter] キーを押します。**

NetVehicle がご購入時の状態で起動します。

```
> logon
# reset clear （下線部入力）
```



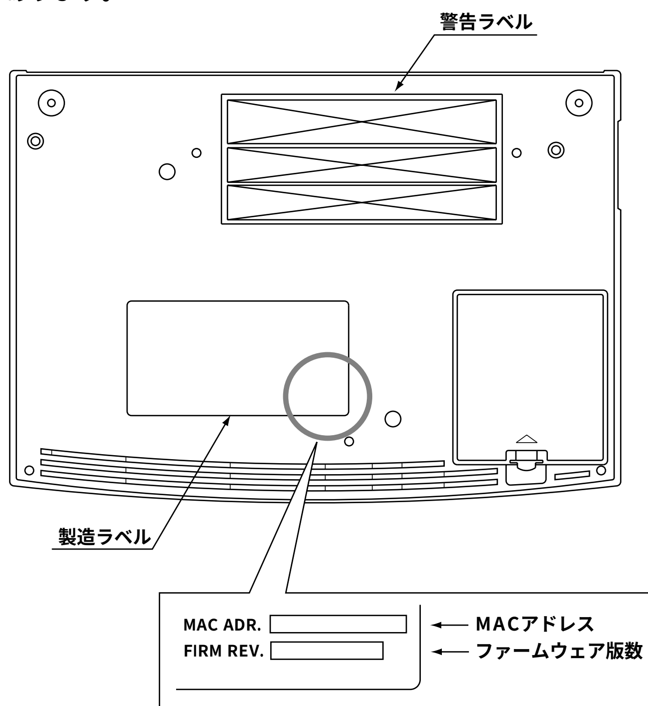
付　録

この章では、
本書で使われている用語や、NetVehicle の仕様などを説明します。



底面のラベルについて

NetVehicle の底面には、警告ラベル、製造ラベル（型名、製造号機、製造日などが記載されるラベル）が貼ってあります。





仕 様

ハードウェア仕様

装置型名		LR50NVL10	
インタフェース	CONSOLE	規格	RS232C
		ポート数	1ポート
		通信速度	9600ビット／秒
		コネクタ	9ピン（DSUB）
	LAN（LAN0）	規格	IEE 802.3u（100BASE−TX／10BASE−T）
		ポート数	1ポート
		通信速度	100Mビット／秒および10Mビット／秒
		コネクタ	8ピン・モジュラジャック（RJ45）
	LAN HUB PORT（LAN1）	規格	IEE 802.3（10BASE−T）
		ポート数	4ポート
		通信速度	10Mビット／秒
		コネクタ	8ピン・モジュラジャック（RJ45）
環境、他	電源／周波数	AC100V 〔50／60Hz〕	
	消費電力	10W	
	外形寸法	278mm（W）× 200mm（D）× 42mm（H）（突起部を除く）	
	重量	約1.0kg	
	温度／湿度	温度： 5〜35℃ 湿度： 10〜90%RH	

ソフトウェア仕様

機能／分類	詳　細
ルーティング対象プロトコル	IP
ルーティングプロトコル	スタティック（128エントリ） ダイナミック（256エントリ） - RIP - RIP2（VLSM対応）
セキュリティ	管理パスワード IPフィルタ　：アドレス／ポート／IN／OUT（最大64）
設定手段	WWWブラウザ　：かんたん設定／詳細設定
ロギング	LAN情報、syslog、DHCP情報、NAT情報
アドレス変換機能	マルチNAT - 動的NAT：最大16個のグローバルIPアドレスが対象、最大1024セッション - 静的NAT：グローバルIPアドレスとポート番号の組み合わせによって最大64個のアドレス変換が可能
簡単／便利機能	DHCPサーバ機能 - DHCPサーバ機能：1つのインタフェースで253台まで - DHCPスタティック機能（※1） DHCPクライアント機能 DHCPリレーエージェント機能 ProxyDNS機能 - DNSサーバ自動切り替え機能（※2） - DNSサーバ機能（※1） URLフィルタ機能（※2） 時刻機能：手動設定、またはTIMEプロトコル／SNTPによる取得 リモートパワーオン機能（WWWブラウザから制御可能）（※1）
レベルアップ	Webワンタッチ／FTPサーバ機能による

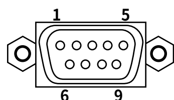
※1）DHCPスタティック+DNSサーバ機能+リモートパワーオン機能で64エントリ登録可能

※2）DNSサーバ自動切り替え機能+URLフィルタ機能で32エントリ登録可能

付録



コンソールポート仕様



コネクタ形状はD-SUB 9ピン－オス
ケーブルはクロス

ピン番号	信号名	方　向	内　容
1	CD	入力	キャリア検出（未使用）
2	RD	入力	受信データ
3	TD	出力	送信データ
4	ER	出力	データ端末レディ
5	GND	－	グランド
6	DR	入力	データセットレディ（未使用）
7	RS	出力	送信要求（未使用）
8	CS	入力	送信可（未使用）
9	CI	入力	呼び出し通知（未使用）

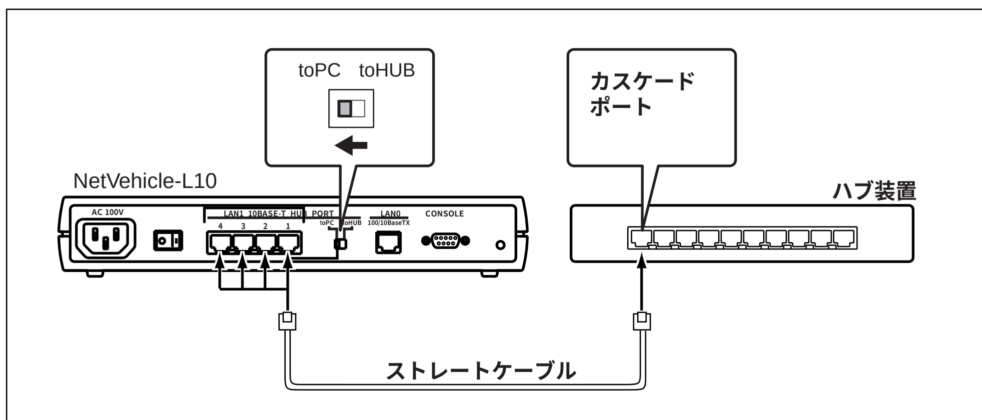


ポート接続形態組み合わせ表

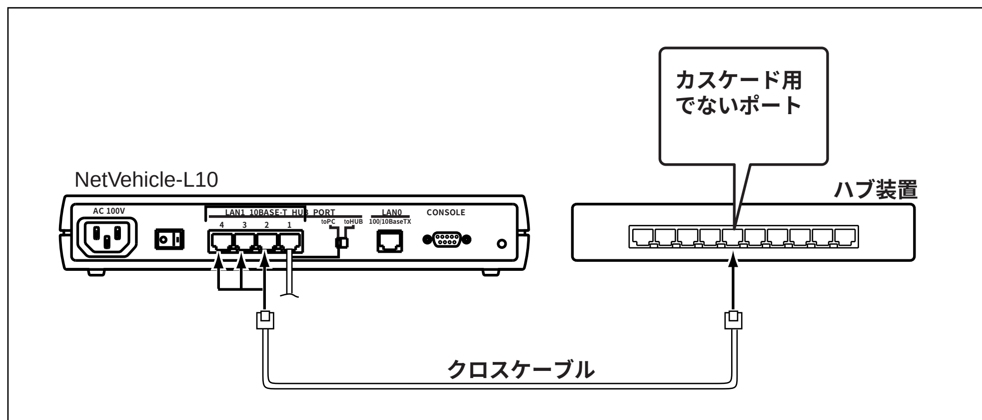
LAN1	切り替えスイッチ	接続装置	接続方法	ケーブルタイプ
ポート1	toPC	パソコン		ストレート
		ハブ	カスケード	ストレート
	toHUB	ハブ	ノーマル	ストレート
ポート2,3,4	―	パソコン		ストレート
	―	ハブ	カスケード	ストレート
	―	ハブ	ノーマル	クロス

ハブとの接続方法

●例1：ハブ装置にカスケードポートがある場合



●例2：NetVehicle のカスケードポートが使われている場合



付
録



用語集

DHCP（Dynamic Host Configularion Protocol）	ネットワーク上のホストに対して、IP アドレスやサブネットマスクなどのネットワーク構成情報を動的に割り当てるための機能です。NetVehicle は、DHCP サーバ機能をサポートしており、DHCP クライアント機能を持っているパソコンに対して、自動的に IP アドレスなどの情報を割り当てることができます。 → DHCP サーバ
DHCP サーバ	DHCP を用いて、IP アドレスなどの設定を配布・管理するシステムです。
DNS（Domain Name System）	IP アドレスとドメイン名を対応させるシステムです。 →ドメイン名、DNS サーバ
DNS サーバ	IP アドレスとドメイン名の対応を管理するコンピュータまたはソフトウェアです。
HUB	→ハブ
IP（Internet Protocol）	通信プロトコルのひとつです。インターネットで標準的に使われています。
IP アドレス	IP による通信（IP ネットワーク）を行う際、ネットワーク上の機器を識別するためのものです。通常は「192.168.1.1」のように、ピリオドをはさんだ 4 つの数字（0 〜 255）で表します。
IP アドレスの静的割り当て	ネットワーク上のホストそれぞれに固有の IP アドレスを割り当てることをいいます。
IP アドレスの動的割り当て	ネットワーク上のホストに、必要に応じて IP アドレスを割り当てることをいいます。
LAN（Local Area Network）	構内回線を使用した狭い地域でのコンピュータ・ネットワークです。局部地域通信網とも呼ばれます。企業内では社内 LAN と呼ばれます。
LAN カード	Ethernet ポートを持たないパソコンを LAN につなぐために使います。
NAT（Network Address Translation）	アドレス変換機能ともいいます。NAT は、プライベートアドレスとグローバルアドレスを変換する機能です。NetVehicle では、NAT 機能を拡張したマルチ NAT もサポートしています。
ping	IP による通信（IP ネットワーク）で、疎通確認をするためのコマンドです。
WWW ブラウザ	HTTP（HyperText Transfer Protocol）を用いて取得した文字、画像などを表示するためのソフトです。主なものとして Netscape Navigator/ Communicator や Microsoft Internet Explorer などがあります。
アドレスマスク	IP アドレスを持ったパソコン、ホスト、サーバなどのネットワークに接続されている装置のグループを表現する時に使用します。アドレスマスクは例えば、あるネットワーク内の端末全部をまとめて表現したい時などに便利な書き方です。このアドレスマスクには、ネットワーク全体を示すためのネットマスクと、ローカルなネットワーク（サブネット）を示すサブネットマスクなどがあります。

また、ネットワークの形状とは無関係にIPアドレスn番からn+m番までの端末を指す場合にも使われます。（ここでnとmは2のべき乗の数になります。）

これらマスク値には“24”などと書きます。これは32bitのIPアドレスの最初の24bit分がマスク値であることを示すものです。また“255.255.255.0”などのようにドット表記で表現する場合もあります。

例えば、192.168.2.0のネットワーク番号はClass Cですからネットマスク値は24（255.255.255.0）です。

ここでサブネットマスクとして26（255.255.255.192）を指定すれば、

① 192.168.2.0 ～192.168.2.63

② 192.168.2.64 ～192.168.2.127

③ 192.168.2.128～192.168.2.191

④ 192.168.2.192～192.168.2.255

の4つサブネットワークが作られます。

さらにここで④のサブネット内の端末のうち、192.168.2.192～192.168.2.207のIPアドレスを持った16台の端末グループを表現したい場合には、アドレスマスク192.168.2.192/28（255.255.255.240）と指定します。

なお、ネットマスクとサブネットマスクは明確な区別なしに使われることも多いようです。本マニュアルではネットマスクとサブネットマスクの両方の意味も含めてネットマスクと呼びます。

カスケード接続	ハブどうしをつなぐことをいいます。
グローバルアドレス	インターネット上のホストを識別するためにInterNICなどのアドレス管理機構から割り当てられる、唯一無二のIPアドレスです。
サブネットマスク	→ネットマスク
詳細設定メニュー	［詳細設定］アイコンをクリックすると、このメニューが表示されます。 このメニューから詳細設定ができます。
操作メニュー	［操作］アイコンをクリックすると、このメニューが表示されます。
ネットマスク	IPアドレスからネットワーク部とホスト部を分離するための区切りを表わします。例えば、IPアドレスが「192.168.1.1」、ネットマスクが「255.255.255.0」の場合、ネットワーク部は「192.168.1」、ホスト部は「1」になります。
ネットワークアドレス	IPアドレスはネットワーク部＋ホスト部で構成されます。 ネットワークアドレスは、ホスト部のビットがすべて0のIPアドレスを意味します。
ネットワーク部	→ネットマスク
ハブ	複数台のパソコンやワークステーションを10BASE-Tケーブルでつないで LANを構築するときに使う装置です。本書では、NetVehicleのハブポートをHUB、別売のハブ装置をハブと表現しています。
表示メニュー	［表示］アイコンをクリックすると、このメニューが表示されます。
ファームウェア	NetVehicleを操作するための内蔵ソフトウェアです。 →メンテナンスメニュー

付録

ブロードキャストアドレス	ネットワーク上のすべてのパソコンに一斉同報する際に使います。 例えば、ホスト部のビットがすべて 1 の IP アドレスや「255.255.255.255」があります。
ホスト部	→ネットマスク
ポート番号	ネットワーク上のサーバやパソコンは、受信したパケットをポート番号によって、アプリケーションを特定します。 例えば、WWW や FTP のようによく知られたアプリケーションには、WWW サーバは 80 番、FTP サーバは 21 番というようにデフォルトの番号が割り当てられています。
メンテナンスメニュー	［メンテナンス］アイコンをクリックすると、このメニューが表示されます。



Q&A

サポート機能について	
Q1.	複数台のパソコンから同時にインターネットにアクセスできますか？
Q2.	NetVehicle の LAN には最大何台のパソコンが接続できますか?
Q3.	どんなプロトコルをサポートしていますか?
Q4.	DHCP とは何ですか?
Q5.	DNS とは何ですか?
Q6.	使用状況 / 稼働状況などを表示できますか?
Q7.	SNMP はサポートしていますか?
NAT（マルチ NAT）について	
Q8.	NATって何ですか?
Q9.	NATってどうやって設定するのですか?
Q10.	（基本 / 静的 / 動的）NAT の違いは何ですか?
Q11.	NAT 機能を使用した場合、FTP が使えなくなるのですか?
Q12.	NAT 機能を使用した場合、UDP アプリケーションは使用できますか?
Q13.	NAT を使っている場合に、IP フィルタリングはどのタイミングで実行されますか?
パソコンの設定について	
Q14.	Windows® 95/98/WindowsNT® で DHCP クライアント機能はどうやれば使えますか?
Q15.	DHCP サーバ機能を利用しない場合、パソコンの設定はどうやればできますか?（Windows® 95/98/WindowsNT®/Macintosh）
Q16.	IP アドレスを設定する場合、使ってはいけない IP アドレスはありますか?
Q17.	ProxyDNS 機能を使用するために必要な設定は？
NetVehicle の設定について	
Q18.	NetVehicle の設定にはどんな WWW ブラウザが使用できますか?
Q19.	IP アドレスを設定する場合、使ってはいけない IP アドレスはありますか?
Q20.	FTP だけデータを通すことはできますか?
Q21.	ポート番号によるフィルタリングはできますか?
Q22.	時刻を設定することはできますか?
セキュリティについて	
Q23.	セキュリティはどうやって確保しますか?
Q24.	特定のパソコンから外部へのネットワークへの接続を禁止することはできますか?
Q25.	特定のパソコンのみ外部のネットワークからアクセスできますか?
Q26.	外部のネットワークから内部のサーバへのアクセスを禁止できますか?
運用について	
Q27.	NetVehicle で使用できるのはどんなパソコンですか?
Q28.	プロキシサーバは使えますか?
Q29.	他の機種で DHCP サーバを動かしているけれど問題ないですか?
Q30.	電源はどうやって切ったら良いですか?
ファームウェアのバージョンアップについて	
Q31.	ファームウェアのバージョンアップ情報はどうやれば入手できますか?
Q32.	ファームウェアのバージョンアップ対応製品と未対応製品では、その後、機能差は出ますか?
Q33.	バージョンアップはどうやればできますか?
Q34.	インターネットに接続していない場合、どうやればバージョンアップできますか?
ログ関連	
Q35.	どんなログを表示できますか?
Q36.	syslog は使えますか?
Q37.	syslog のファシリティは何ですか?
Q38.	syslog でどんな情報（プライオリティ）が入手できますか?
10BASE-T ハブについて	
Q39.	5 台以上のパソコンをハブポートにつなげられますか?
通信について	
Q40.	10BASE-T 以外（10BASE-5 または 10BASE-2 など）を使用した環境で通信が極端に遅い、または通信できない。
Q41.	NetVehicle の IP アドレスを「DHCP サーバから取得する」から「指定する」に変更したら、通信できなくなった。

付
録

サポート機能について

Q1. 複数台のパソコンから同時にインターネットにアクセスできますか?

A. できます。アクセス可能な台数は使用形態により異なります。

NAT 使用形態	同時接続制限
使わない	ネットワークのすべての端末
基本 NAT	割り当てられたグローバル IP アドレスの数
動的 NAT	最大 1024 セッション
静的 NAT	最大 1024 セッション + マッピングした情報数

Q2. NetVehicle の LAN には最大何台のパソコンが接続できますか?

A. ネットワークのルールに従えば、接続台数の制限はありません。

ネットワークのルールに従ってください。例えば、192.168.1.0/255.255.255.0 のネットワークであった場合、192.168.1.1 ～ 192.168.1.254 の 254 台のうち、NetVehicle の 1 台分を差し引いた 253 台までのパソコンが接続できます。

補足 NetVehicle の DHCP サーバ機能を利用すると、最大 253 台まで IP アドレスなどの情報を自動的に割り当てられます。254 台以上パソコンがある場合は、254 台目から IP アドレスなどの情報をそれらに個別に設定してください。

Q3. どんなプロトコルをサポートしていますか?

A. インターネットプロトコル(IP)をサポートしています。

IP(Internet Protocol)は、その名のとおりインターネットで通信を行うためのプロトコルです。インターネットに接続する場合には、このプロトコルが必要不可欠です。AppleTalk、IPX/SPX、FNA、SNA など、IP 以外の通信プロトコルではご使用いただけません。

Q4. DHCP とは何ですか?

A. DHCP(Dynamic Host Configuration Protocol)は、IP アドレスなどの情報を割り当てるためのプロトコルです。

これを使用することにより、管理元(DHCP サーバ)から各パソコン(DHCP クライアント)に対し、IP アドレスやゲートウェイアドレスなどネットワークの各種設定を自動化できます。ネットワーク環境が変化した場合でも、管理元の設定を変更することでパソコン側の設定も変更できます。NetVehicle には DHCP サーバ機能が搭載されています。(P.84)

Q5. DNS とは何ですか?

A. DNS(Domain Name System)は、ホスト名(あるいは端末名)と IP アドレスを管理するデータベースです。

DNS にアクセスすることによって、そこに登録されている世界中のアドレス情報を取り出すことができます。例えば、よく使われている WWW ブラウザや e-mail で表記されるホスト名(例えば、www.fujitsu.co.jp、ftp.fujitsu.co.jp)はこのデータベースを使い、IP アドレスに変換されます。WWW ブラウザなどのアプリケーションは検索してきた結果(IP アドレス)を利用して通信することができるようになります。

Q6. 使用状況 / 稼働状況などを表示できますか?

A. www ブラウザを使って表示 / 出力ができます。

表示メニュー(P.115)で表示できる情報は WWW ブラウザを介して表示 / 出力ができます。

Q7. SNMP はサポートしていますか?

A. サポートしていません。

NAT（マルチ NAT）について

Q8. NAT とは何ですか?

A. Network Address Translation の略です。

簡単に言えば、NetVehicle と同じ LAN につながっているパソコンの IP アドレスが、NetVehicle を通ってインターネットに出て行く時に、違う IP アドレスになって出て行く機能です。
NetVehicle では NAT 機能を拡張したマルチ NAT をサポートしています。

Q9. NATってどうやって設定するのですか?

A. 詳細設定の LAN0/LAN1 情報から行います。（P.58）

かんたん設定でプライベート LAN 構築を選んだ場合、動的 NAT が設定されます。それ以外で NAT 機能を利用する場合は、必ず詳細設定で設定する必要があります。

Q10.（基本 / 静的 / 動的）NAT の違いは何ですか?

A. 同時接続できる台数、機能制限に以下のような違いがあります。

NATの種類	同時接続制限（セッション数）	備考
基本NAT	割り当てIPアドレス数	割り当て時間内は外部を起点とした通信も可能
動的NAT	1024セッション	外部を起点とした通信は不可能
静的NAT	1024セッションとマッピングした情報	プライベートアドレス（とポート）をグローバルアドレス（とポート）にマッピングできる／マッピングしたアドレスに関しては、外部を起点とした通信も可能

Q11. NAT 機能を使用した場合、FTP が使えなくなるのですか?

A. NetVehicle の NAT 機能ならば大丈夫です。

本来の NAT 機能の場合、IP 通信の要となる IP ヘッダ（葉書などの住所 / 郵便番号）部分に書き込まれているプライベートアドレスをグローバルアドレス（またはその逆）に変換する機能です。
しかし FTP の場合、パソコンが IP ヘッダの上位層（葉書でいうと文章）でローカル IP アドレス（住所）を伝え、サーバは教えられた“ ローカル IP アドレス（プライベートアドレス）”にデータを送信しますが、存在しない（あるいは存在してもサービスを望んでいない）ため、通信は失敗に終わります。
そこで NetVehicle の NAT 機能は、FTP 通信を見つけると上位層のローカル IP アドレス（プライベートアドレス）をグローバルアドレスに書換えて正しく通信できるようにしています。

Q12. NAT機能を使用した場合、UDPアプリケーションは使用できますか?

A. StreamWorks、RealPlayer、VDOLiveなどが利用できます。

UDP通信はTCP通信と違い、コネクション確立を行わない通信です。このため、大量データ転送を送り込む動画転送アプリケーション（RealAudioなど）に使用されます。
一般的なNAT機能を利用している場合、ローカルIPアドレス（プライベートアドレス）とグローバルアドレスが1対1に対応しないため、外部を起点とした通信は行えません。このため、動画などのサーバを通信起点としたUDPアプリケーションには本来対応できません。
しかし、NetVehicleのNAT機能は、ローカルIPアドレス（プライベートアドレス）とグローバルアドレスが1対1に対応しているため、StreamWorks、RealPlayer、VDOLiveには対応しています。また、マルチNAT機能（“基本NAT”または“静的NAT”）を使用することで、複数端末が同時に外部接続し、UDPアプリケーションは特定の1台または割り当てられているグローバルアドレスの数の端末で楽しめます。
ただし、インターネットホンの類はご使用いただけません。インターネットホンもftpと同様、上位層でローカルIPアドレス（プライベートアドレス）をサーバに送出しているアプリケーションであり、なおかつ、データのやりとりのしくみが非公開であるため、対応ができまません（インターネットホンはアプリケーション間で互換性がない場合が多く、また、独自仕様の通信を行っています）。

［NetVehicleのインターネットホンへの対応状況］
- Microsoft NetMeetingの音声/画像通信は利用不可（ただしチャットは可能）
- CU SeeMeは利用可能

上記以外は未確認です。

Q13. NATを使っている場合、IPフィルタリングはどのタイミングで実行されますか?

A. プライベートアドレスを使って行われます。

内部LANから外部LANに向かう場合は、NAT機能でアドレスが変更される前にフィルタリング対象であるかどうかをチェックします。また、外部LANから内部LANに向かう場合は、NAT機能でアドレス変換されたあとでフィルタリング対象であるかどうかをチェックします。

パソコンの設定について

Q14. Windows® 95/98/Me、WindowsNT®、MacintoshでDHCPクライアント機能はどうやれば使えますか?

A. 製品に添付されているマニュアルを参照してください。（P.24）

Q15. DHCPサーバ機能を利用しない場合、パソコンの設定はどうやればできますか?（Windows® 95/98/Me、WindowsNT®、Macintosh）

A. 商品に添付されているマニュアルを参照してください。

Q16. IP アドレスを設定する場合、使ってはいけない IP アドレスはありますか?

A. 次の 3 種類の IP アドレスを使ってはいけません。

- すでに使用されている IP アドレス
  IP ネットワークでは、IP アドレスが世界中で必ず 1 つであることを条件に構成されています。プライベートアドレスを使って接続する端末型接続の場合でも、NAT 機能を用いて世界中で一つしかない IP アドレスに変換します。
- ネットワークアドレスを示す IP アドレス（0 ブロードキャスト）
  ネットワーク部（そのまま）+ ホスト部のビットがすべて 0 の IP アドレス
- ブロードキャストアドレスを示す IP アドレス（1 ブロードキャスト）
  ネットワーク部（そのまま）+ ホスト部のビットがすべて 1 の IP アドレス

Q17. ProxyDNS 機能を使用するために必要な設定は？

A. ProxyDNS機能を使用するには、LAN上のパソコンがNetVehicleのIPアドレスをDNSサーバのアドレスとして認識しなくてはなりません。

- パソコンが DHCP クライアントである場合
  DHCP サーバに NetVehicle の IP アドレスを DNS サーバとして広報するように設定します。
  NetVehicleがDHCPサーバになっている場合は、かんたん設定（プライベートLAN構築）の［LAN1］もしくは詳細設定の［DHCP 機能］で DNS サーバ広報を設定する必要があります。
- パソコンが DHCP クライアントではない場合
  パソコンに DNS サーバのアドレスとして NetVehicle の IP アドレスを設定します。
  ここでは、Windows® 98 の場合を例に説明します。
  ①「コントロールパネル」ウィンドウで「ネットワーク」アイコンをダブルクリックします。
  ②「ネットワーク」ウィンドウで［ネットワークの設定］タブをクリックします。
  ③ 一覧から「TCP/IP」を選択し、［プロパティ］ボタンをクリックします。
  ④「TCP/IP のプロパティ」画面で［DNS 設定］タブをクリックします。
  ⑤「DNS を使う」を選択します。
  ⑥「DNS サーバの検索順」ダイアログボックスに、NetVehicle の IP アドレスを入力します。

補足 必要に応じて、ホスト名にパソコンの名前（任意）を入力します。

付録

NetVehicle の設定について

Q18. NetVehicle の設定にはどんな WWW ブラウザが使用できますか?

A. Netscape Navigator Version 3.0 以降（ただし Netscape6 を除く）と Microsoft Internet Explorer Version 4.0 以降です。

Microsoft Internet Explorer Version 3.0 で NetVehicle の設定を行うと、設定した情報が正しく設定されないことがあります。

Q19. IP アドレスを設定する場合、使ってはいけないIP アドレスはありますか?

A. 次の 3 種類のIP アドレスは使わないでください。

- すでに使用されているIP アドレス
  IP ネットワークでは、IP アドレスが世界中で必ず 1 つであることを条件に構成されています。プライベートアドレスを使って接続する端末型接続の場合でも、NAT機能を用いて世界中で一つしかないIP アドレス（グローバルアドレス）に変換します。
- ネットワーク部を示すIP アドレス（0 ブロードキャスト）
  ネットワーク部（そのまま）+ ホスト部がすべて 0（2 進数表記）のIP アドレス
- ブロードキャストアドレスを示すIP アドレス（1 ブロードキャスト）
  ネットワーク部（そのまま）+ ホスト部がすべて 1（2 進数表記）のIP アドレス

ネットワーク部 / ホスト部の求めかたは以下のとおりです。

ネットワーク部 =IP アドレス & ネットマスク（論理積）
ホスト部 =IP アドレス &（not ネットマスク）（論理積と排他）

例えば、NetVehicle のデフォルトIP アドレスである、192.168.1.1/255.255.255.0（24bit）の場合、ネットワーク部 / ホスト部は以下のとおりです。

ネットワーク部

```
192.168.1.1      =  11000000.10101000.00000001.00000001
&255.255.255.0   =  11111111.11111111.11111111.00000000
192.168.1.0      =  11000000.10101000.00000001.00000000
```

ホスト部

```
192.168.1.1      =  11000000.10101000.00000001.00000001
&255.255.255.0   =  00000000.00000000.00000000.11111111
0.0.0.1          =  00000000.00000000.00000000.00000001
```

この場合、以下のようになります。

NetVehicle のIP アドレス =192.168.1.1（ホスト部:00000001）
ネットワークアドレス =192.168.1.0（ホスト部:00000000）
ブロードキャストアドレス =192.168.1.255（ホスト部:11111111）

Q20. FTP だけデータを通すことはできますか?

A. IP フィルタリング機能を使えばできます。（P.69）

Q21. ポート番号によるフィルタリングはできますか?

A. できます。

NetVehicle のIP フィルタリングは、IP アドレス / ポート番号 /TCP 接続要求を対象にするか（TCP のみ）などの設定が可能です。フィルタリング動作としては、透過 / 遮断があります。

Q22. 時刻を設定することはできますか？

A. 端末から時刻を取得、タイムサーバから時刻を取得、または任意の時刻を設定の 3 通りの方法で設定できます。

- 操作メニューの「時刻設定」でパソコンから時刻を取得、または任意の時刻を設定することができます。
- 詳細設定メニューの「装置情報」クリックし、「装置情報設定」ページの［タイムサーバ情報］の設定で、「使用する」を選択し、かつ、「プロトコル」「タイムサーバIP アドレス」「自動時刻設定間隔」を設定すると、NetVehicleからの時刻問い合わせにより自動的に時刻を合わせます。また、［タイムサーバ情報］が設定されている場合、操作メニューの「時刻設定」にて、「タイムサーバからの時刻を取得」の［設定］ボタンをクリックすることによって、即時に取得することもできます。

セキュリティについて

ここでは、便宜上、セキュリティを確保したい LAN 側を内部、それ以外を外部と定義します。

Q23. セキュリティはどのように確保しますか?

A. NAT、IP フィルタリングなどの機能で確保できます。（P.64、P.69）

- NAT 機能を使用する
  NetVehicle を使用して LAN0 側と LAN1 側の IP アドレスを変換して、LAN0 側または LAN1 側のアドレスを見えなくします。
- IP フィルタリング機能を使用する
  特定の IP アドレスのみ透過（または遮断）し、不要な通信を遮断できます。
- 管理者パスワードを設定する。

Q24. 特定のパソコンから外部のネットワークへの接続を禁止することはできますか?

A. IP フィルタリング機能を使うことで実現可能です。

例えば、192.168.1.3からNetVehicleを使用して外部のネットワークへの接続を禁止する場合の設定内容は以下のようになります。

プロトコル	すべて
動作	遮断
IP アドレス	192.168.1.3
アドレスマスク	255.255.255.255

Q25. 特定のパソコンのみ外部のネットワークからアクセスできますか?

A. IP フィルタリング機能を使うことで実現可能です。

例えば、192.168.1.0/24 のネットワークの 192.168.1.3 へのアクセスを許す場合の設定内容は以下のようになります。

[優先順位 1]

プロトコル	すべて
動作	透過
IP アドレス	192.168.1.3
アドレスマスク	255.255.255.255

[優先順位 2]

プロトコル	すべて
動作	遮断
IP アドレス	192.168.1.0
アドレスマスク	255.255.255.0

Q26. 外部のネットワークから内部のサーバへのアクセスを禁止できますか?

A. NAT 機能を利用することで、実現可能です。

NAT 機能は NetVehicle を介して外部のネットワークにアクセスするときに、元の IP アドレス（プライベートアドレス）を違う IP アドレス（グローバルアドレス）に振り替えて外部のネットワークのサーバと通信するための機能です。
パソコンの IP アドレス（プライベートアドレス）を、違う IP アドレス（グローバルアドレス）に変換して通信するため、内部から外部にアクセスできても、外部から内部にアクセスできません。(IP アドレスの変換テーブルに変換情報がないため)
IP フィルタリング機能を使って細かい設定をすることなく、外部からのアクセスを止められます。

運用について

Q27. NetVehicle で使用できるのはどんな端末ですか?

A. 次の条件がそろっていれば、パソコン、ワークステーションはほとんどご使用いただけます。

- Ethernet ポート、または Ethernet アダプタを備えている。
- IP プロトコルをサポートしている。

Q28. プロキシサーバは使えますか?

A. ご使用いただけます。

設定方法は、お使いのブラウザによって違います。「noProxy」や「Proxy サーバを使わない」などの項目に NetVehicle の IP アドレスを設定し、NetVehicle のみプロキシサーバを使わない設定にしてください。

- Netscape Communicator 4.7 の場合は、次のように設定します。
  ①「編集」メニューから「設定」を選択する。
  ②設定画面の「カテゴリ」で「詳細－プロキシ」を選択する。
  ③「手動でプロキシを設定する」を選択し、[表示] ボタンをクリックする。
  ④「HTTP」にプロバイダの Proxy サーバを指定します。
  ⑤例外の「次ではじまるドメインにはプロキシサーバを使用しない」に NetVehicle の IP アドレス（192.168.1.1）を指定する。
- Microsoft Inernet Explorer 5.5 の場合は、次のように設定します。
  ①［ツール］メニューから「インターネットオプション」を選択する。
  ② インターネットオプション画面の「接続」タブで、LAN の設定の「LAN の設定」ボタンをクリックする。
  ③プロキシサーバーの「プロキシサーバーを使用する」が選択されていることを確認し、[詳細] ボタンをクリックする。
  ④「HTTP」にプロバイダの Proxy サーバを指定する。
  ⑤例外の「次で始まるアドレスにはプロキシを使用しない」にNetVehicleのIPアドレス（192.168.1.1）を指定する。

Q29. 他の機種で DHCP サーバを動かしているけれど問題ないですか？

A. NetVehicle の DHCP サーバ機能は使用しないでください。

NetVehicle の DHCP サーバ機能より、UNIX サーバや WindowsNT サーバなど他の機種の方が、より細かい情報をパソコンに割り当てることができます。NetVehicle の DHCP サーバ機能は停止して、既存の DHCP サーバをそのまま使用されることをお勧めします。

Q30. 電源はどうやって切ったら良いですか?

A. 通常運用では電源スイッチをそのまま切っていただいても、NetVehicle本体には影響を与えません。

⚠注意

ファームウェアのバージョンアップ作業を行っている場合は絶対に電源を切らないでください。

ファームウェアのバージョンアップについて

Q31. ファームウェアのバージョンアップ情報はどうやれば入手できますか?

A. バージョンアップ情報は NetVehicle サポートページで広報します。

NetVehicle のサポートページ（http://telecom.fujitsu.com/jp/products/nv/）では、バージョンアップ時期以外にも、追加・拡張された機能を紹介していきます。定期的にご覧ください。

Q32. ファームウェアのバージョンアップ対応製品と未対応製品では、その後、機能差は出ますか?

A. **バージョンアップを行っていただければ、同一機種ならば機能差はありません。**
例えば、バージョンアップ対応製品が出荷されたあとでも、それ以前から店頭に並んでいる商品は旧バージョンの可能性があります。そのような製品を購入された場合にも、ファームウェアをバージョンアップしていただくことで機能を拡張できます。

Q33. バージョンアップはどうやればできますか?

A. **NetVehicle がインターネットに接続されていればできます。（P.116）**

Q34. インターネットに接続していない場合、どうやればバージョンアップできますか？（FTP サーバより最新ファームウエアをダウンロードする方法）

A. **以下の２つの方法があります。**

- FTP サーバより最新のファームウェアをダウンロードする方法
- FTP クライアントより最新ファームウェアを転送する方法

[FTP サーバより最新ファームウェアをダウンロードする方法]

1）FTP サーバを準備します。
UNIX サーバをお持ちの方は適当なユーザを作っていただければ可能です。Windows® ９５の場合、Microsoft 社が提供しているパーソナルウェブサーバを利用すると簡単です。

2）最新ファームウェアを入手します。
ニフティサーブのインターネット接続サービスを利用してNetVehicle用のファームウェアを入手する場合は、以下の手順で行います。

ニフティサーブ接続後の画面表示の例

```
＞GO  INTERNET
インターネット INTERNET
1. インターネットについて
2. 利用方法
3.Q&A コーナー
4.NIFTYMANAGER と WWW ブラウザー
5.ftp
6.fj/tnn news group（netnews）
7.telnet
8. フォーラム／ステーション
9. インターネットパイロットコーナー
＞5

ftp FTP
1. ご案内／利用方法
2.archie
3.anonymous ftp
4.ftp
＞3

anonymous ftp AFTP
1. 任意のサイトに入る
2.ftp.web.ad.jp に入る
3.ftp.iij.ad.jp に入る
＞1

ホスト名（ドメイン名又は URL 例:ftp://ftp.web.ad.jp/pub/README）：
          ftp://ftp.fujitsu.co.jp/pub/NV/firm/L10SOFT.ftp
ホスト名：ftp.fujitsu.co.jp
ファイル名：/pub/NV/firm/L10SOFT.ftp
```

付録

3）LAN 上の FTP サーバに、入手したファイルを置く。
同一のファイル名にしておくと便利です。ここでのファイル名は「/pub/NV/firm/L10SOFT.ftp」です。

4）NetVehicle の「ファームウェア更新情報」に LAN 上の FTP サーバを設定する。
① 設定メニューで「詳細設定」の「装置情報」をクリックします。
② 「装置情報設定」ページの［ファームウェア更新情報］の中の「転送元ホスト名」に、ftp サーバの IP アドレスを入力します。
③ 「ファイルロケーション」（ファイル名も含む）を変更した場合、正しいことを確認してください。
④ ［更新］ボタンをクリックします。
⑤ ［設定反映］ボタンをクリックします。

5）ファームウェアを更新する。
① ［メンテナンス］アイコンをクリックします。
② メンテナンスメニューで「ファームウェア更新」をクリックします。
③ 設定内容表示ページが表示されたら、内容に間違いがないことを確認して［OK］ボタンをクリックします。
④ここからバージョンアップ処理が行われます。
（バージョンアップ中には電源を切らないように注意してください。）
⑤ バージョンアップ終了を告げるメッセージが表示されると完了です。

[ftp クライアントにより最新ファームウェアを転送する方法]

NetVehicle の FTP サーバ機能を使って最新ファームを転送する方法です。
本書の説明を参考にバージョンアップを行ってください。（P.122）

ログ関連

Q35. どんなログを表示できますか?

A. 次のログが見られます。

[表示メニューで確認できる内容]（P.115）

- DHCP 情報　：使用している IP アドレスなどの情報を確認できます。
- NAT 情報　：NAT のセッションの状態を確認できます。
- ルーティング情報　：ルーティングテーブルを確認できます。
- IP 統計情報　：ルーティングシタ通信のプロトコルを確認できます。
- LAN 情報　：LAN の統計情報を確認できます。
- VPN 情報　：VPN 情報を確認できます。
- システムログ　：システム運用状況の履歴が確認できます。
- 現在時刻　：現在時刻を確認できます。
- 経過時間情報　：電源投入後、経過した時間を確認できます。

[メンテナンスメニューで確認できる内容]（P.117）

- バージョン情報　：エラーログ情報　構成定義情報　ファームウェアの更新
- バージョン情報　：ファームウェアバージョンを表示します。
- エラーログ情報　：エラーログが表示されます。
- 構成定義情報　：構成定義情報が表示されます。

Q36. syslog は使えますか?

A. 使えます。システムログを設定できます。

Q37. syslog のファシリティは何ですか？

A. 23（個人が割り当て出来る数）が設定されます。

Q38. syslog でどんな情報（プライオリティ）が入手できますか？

A. 次の情報が入手できます。

- LOG_ERR　エラーメッセージ
- LOG_WARN　警告メッセージ
- LOG_NOTICE　エラー以外のシステムメッセージ
- LOG_INFO　上記以外のお知らせ

10BASE-T ハブについて

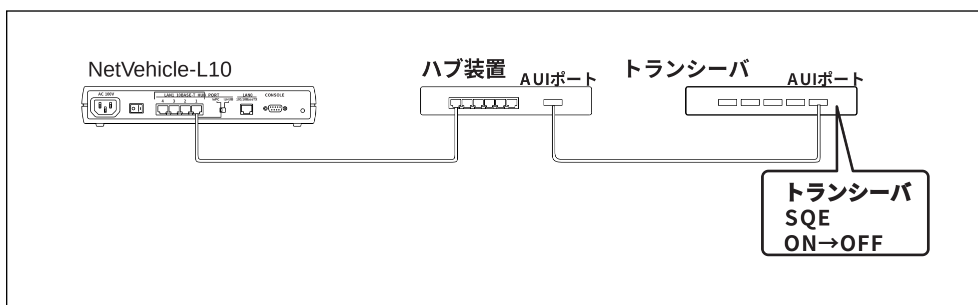
Q39. 5 台以上のパソコンをハブポートにつなげられますか？

A. ハブ装置を増設することによりつなげられます。（P.39）

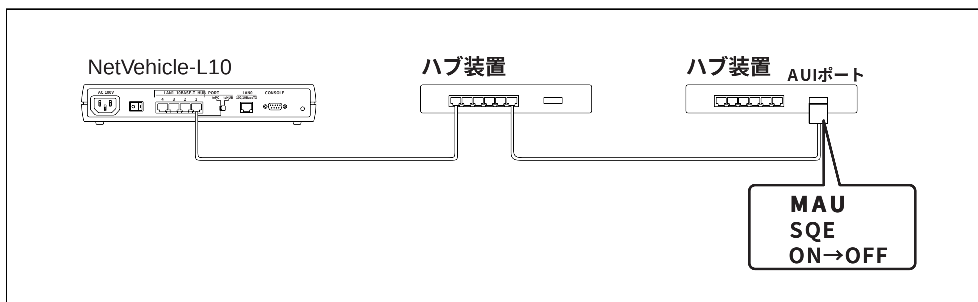
Q40. 10BASE-T 以外（10BASE-5 または 10BASE-2 など）を使用した環境で通信が極端に遅い、または通信できない。どうすればよいか？

A. NetVehicle を接続した LAN に接続されている MAU（*1）の設定または 10BASE-5/10BASE-2 トランシーバの SQE（*2）設定が誤っている可能性があります。MAU または10BASE-5/10BASE-2トランシーバが以下のように接続されていないか確認してください。

【例 1】
10BASE-5/10BASE-2 トランシーバの AUI ポートと ハブ装置の AUI ポートを接続している場合は、10BASE-5/10BASE-2 トランシーバの SQE テストがON になっていないか確認し、SQE テスト OFF の設定にします。



【例 2】
2 台のハブ装置を ハブ装置の AUIポート（*3）に接続されている MAU経由で行う場合は、MAUの SQE テストが ON になっていないか確認し、SQE テスト OFF の設定にします。




こんな事に気をつけて

SQE テストの設定が行えないトランシーバの AUI ポートの場合は、端末（パソコン）接続専用のためハブ装置を直接接続できません。

*1)　10BASE-T ポート <->AUI ポート変換コネクタ
*2)　トランシーバの自己診断機能
*3)　10BASE-5 接続コネクタポート

Q41. NetVehicle の IP アドレスを「DHCP サーバから取得する」から「指定する」に変更したら、通信できなくなった。どうすればよいか？

A. DHCPサーバから自動的に受け取っていたデフォルトルータのIPアドレス情報が受け取れなくなったので、［スタティック情報一覧］のデフォルトルータを設定してください。



MIB 一覧

NetVehicle の SNMP エージェント機能でサポートする MIB の一覧を示します。

system グループ

MIB	OID	SYNTAX	ACCESS
sysDescr	system.1	DisplayString	R
sysObjectID	system.2	OBJECT ID	R
sysUpTime	system.3	TimeTicks	R
sysContact	system.4	DisplayString	R
sysName	system.5	DisplayString	R
sysLocation	system.6	DisplayString	R
sysServices	system.7	INTEGER	R

interface グループ

MIB	OID	SYNTAX	ACCESS
ifNumber	interfaces.1	INTEGER	R
ifTable	interfaces.2	Aggregate	NA
ifEntry	ifTable.1	Aggregate	NA
ifIndex	ifEntry.1	INTEGER	R
ifDescr	ifEntry.2	DisplayString	R
ifType	ifEntry.3	INTEGER	R
ifMtu	ifEntry.4	INTEGER	R
ifSpeed	ifEntry.5	Gauge	R
ifPhysAddress	ifEntry.6	PhysAddress	R
ifAdminStatus	ifEntry.7	INTEGER	R
ifOperStatus	ifEntry.8	INTEGER	R
ifLastChange	ifEntry.9	TimeTicks	R
ifInOctets	ifEntry.10	Counter	R
ifInUcastPkts	ifEntry.11	Counter	R
ifInNUcastPkts	ifEntry.12	Counter	R
ifInDiscards	ifEntry.13	Counter	R
ifInErrors	ifEntry.14	Counter	R
ifInUnknownProtos	ifEntry.15	Counter	R
ifOutOctets	ifEntry.16	Counter	R
ifOutUcastPkts	ifEntry.17	Counter	R
ifOutNUcastPkts	ifEntry.18	Counter	R
ifOutDiscards	ifEntry.19	Counter	R
ifOutErrors	ifEntry.20	Counter	R
ifOutQLen	ifEntry.21	Gauge	R
ifSpecific	ifEntry.22	OBJECT ID	R

address translation グループ

MIB	OID	SYNTAX	ACCESS
atTable	at.1	Aggregate	NA
atEntry	atTable.1	Aggregate	NA
atIfIndex	atEntry.1	INTEGER	R
atPhysAddress	atEntry.2	PhysAddress	R
atNetAddress	atEntry.3	NetworkAddress	R

付録

ip グループ

MIB	OID	SYNTAX	ACCESS
ipForwarding	ip.1	INTEGER	R
ipDefaultTTL	ip.2	INTEGER	R
ipInReceives	ip.3	Counter	R
ipInHdrErrors	ip.4	Counter	R
ipInAddrErrors	ip.5	Counter	R
ipForwDatagrams	ip.6	Counter	R
ipInUnknownProtos	ip.7	Counter	R
ipInDiscards	ip.8	Counter	R
ipInDelivers	ip.9	Counter	R
ipOutRequests	ip.10	Counter	R
ipOutDiscards	ip.11	Counter	R
ipOutNoRoutes	ip.12	Counter	R
ipReasmTimeout	ip.13	INTEGER	R
ipReasmReqds	ip.14	Counter	R
ipReasmOKs	ip.15	Counter	R
ipReasmFails	ip.16	Counter	R
ipFragOKs	ip.17	Counter	R
ipFragFails	ip.18	Counter	R
ipFragCreates	ip.19	Counter	R
ipAddrTable	ip.20	Aggregate	NA
ipAddrEntry	ipAddrTable.1	Aggregate	NA
ipAdEntAddr	ipAddrEntry.1	IpAddress	R
ipAdEntIfIndex	ipAddrEntry.2	INTEGER	R
ipAdEntNetMask	ipAddrEntry.3	IpAddress	R
ipAdEntBcastAddr	ipAddrEntry.4	INTEGER	R
ipAdEntReasmMaxSize	ipAddrEntry.5	INTEGER	R
ipRouteTable	ip.21	Aggregate	NA
ipRouteEntry	ipRouteTable.1	Aggregate	NA
ipRouteDest	ipRouteEntry.1	IpAddress	R
ipRouteIfIndex	ipRouteEntry.2	INTEGER	R
ipRouteMetric1	ipRouteEntry.3	INTEGER	R
ipRouteMetric2	ipRouteEntry.4	INTEGER	R
ipRouteMetric3	ipRouteEntry.5	INTEGER	R
ipRouteMetric4	ipRouteEntry.6	INTEGER	R
ipRouteNextHop	ipRouteEntry.7	IpAddress	R
ipRouteType	ipRouteEntry.8	INTEGER	R
ipRouteProto	ipRouteEntry.9	INTEGER	R
ipRouteAge	ipRouteEntry.10	INTEGER	R
ipRouteMask	ipRouteEntry.11	IpAddress	R
ipRouteMetric5	ipRouteEntry.12	INTEGER	R
ipRouteInfo	ipRouteEntry.13	OBJECT ID	R
ipNetToMediaTable	ip 22	Aggregate	NA
ipNetToMediaEntry	ipNetToMediaTable.1	Aggregate	NA
ipNetToMediaIfIndex	ipNetToMediaEntry.1	INTEGER	R
ipNetToMediaPhysAddress	ipNetToMediaEntry.2	PhysAddress	R
ipNetToMediaNetAddress	ipNetToMediaEntry.3	IpAddress	R
ipNetToMediaType	ipNetToMediaEntry.4	INTEGER	R
ipRoutingDiscards	ip 23	Counter	R
ipForward	ip 24	Aggregate	NA
ipForwardNumber	ipForward.1	Gauge	R
ipForwardTable	ipForward.2	Aggregate	NA
ipForwardEntry	ipForwardTable.1	Aggregate	NA
ipForwardDest	ipForwardEntry.1	IpAddress	R
ipForwardMask	ipForwardEntry.2	IpAddress	R
ipForwardPolicy	ipForwardEntry.3	INTEGER	R
ipForwardNextHop	ipForwardEntry.4	IpAddress	R
ipForwardIfIndex	ipForwardEntry.5	INTEGER	R
ipForwardType	ipForwardEntry.6	INTEGER	R
ipForwardProto	ipForwardEntry.7	INTEGER	R
ipForwardAge	ipForwardEntry.8	INTEGER	R
ipForwardInfo	ipForwardEntry.9	OBJECT ID	R
ipForwardNextHopAS	ipForwardEntry.10	INTEGER	R
ipForwardMetric1	ipForwardEntry.11	INTEGER	R
ipForwardMetric2	ipForwardEntry.12	INTEGER	R
ipForwardMetric3	ipForwardEntry.13	INTEGER	R
ipForwardMetric4	ipForwardEntry.14	INTEGER	R
ipForwardMetric5	ipForwardEntry.15	INTEGER	R

icmp グループ

MIB	OID	SYNTAX	ACCESS
icmpInMsgs	icmp.1	Counter	R
icmpInErrors	icmp.2	Counter	R
icmpInDestUnreachs	icmp.3	Counter	R
icmpInTimeExcds	icmp.4	Counter	R
icmpInParmProbs	icmp.5	Counter	R
icmpInSrcQuenchs	icmp.6	Counter	R
icmpInRedirects	icmp.7	Counter	R
icmpInEchos	icmp.8	Counter	R
icmpInEchoReps	icmp.9	Counter	R
icmpInTimestamps	icmp.10	Counter	R
icmpInTimestampReps	icmp.11	Counter	R
icmpInAddrMasks	icmp.12	Counter	R
icmpInAddrMaskReps	icmp.13	Counter	R
icmpOutMsgs	icmp.14	Counter	R
icmpOutErrors	icmp.15	Counter	R
icmpOutDestUnreachs	icmp.16	Counter	R
icmpOutTimeExcds	icmp.17	Counter	R
icmpOutParmProbs	icmp.18	Counter	R
icmpOutSrcQuenchs	icmp.19	Counter	R
icmpOutRedirects	icmp.20	Counter	R
icmpOutEchos	icmp.21	Counter	R
icmpOutEchoReps	icmp.22	Counter	R
icmpOutTimestamps	icmp.23	Counter	R
icmpOutTimestampReps	icmp.24	Counter	R
icmpOutAddrMasks	icmp.25	Counter	R
icmpOutAddrMaskReps	icmp.26	Counter	R

tcp グループ

MIB	OID	SYNTAX	ACCESS
tcpRtoAlgorithm	tcp.1	INTEGER	R
tcpRtoMin	tcp.2	INTEGER	R
tcpRtoMax	tcp.3	INTEGER	R
tcpMaxConn	tcp.4	INTEGER	R
tcpActiveOpens	tcp.5	Counter	R
tcpPassiveOpens	tcp.6	Counter	R
tcpAttemptFails	tcp.7	Counter	R
tcpEstabResets	tcp.8	Counter	R
tcpCurrEstab	tcp.9	Gauge	R
tcpInSegs	tcp.10	Counter	R
tcpOutSegs	tcp.11	Counter	R
tcpRetransSegs	tcp.12	Counter	R
tcpConnTable	tcp.13	Aggregate	NA
tcpConnEntry	tcpConnTable.1	Aggregate	NA
tcpConnState	tcpConnEntry.1	INTEGER	R
tcpConnLocalAddress	tcpConnEntry.2	IpAddress	R
tcpConnLocalPort	tcpConnEntry.3	INTEGER	R
tcpConnRemAddress	tcpConnEntry.4	IpAddress	R
tcpConnRemPort	tcpConnEntry.5	INTEGER	R
tcpInErrs	tcp.14	Counter	R
tcpOutRsts	tcp.15	Counter	R

udp グループ

MIB	OID	SYNTAX	ACCESS
udpInDatagrams	udp.1	Counter	R
udpNoPorts	udp.2	Counter	R
udpInErrors	udp.3	Counter	R
udpOutDatagrams	udp.4	Counter	R
udpTable	udp.5	Aggregate	NA
udpEntry	udpTable.1	Aggregate	NA
udpLocalAddress	udpEntry.1	IpAddress	R
udpLocalPort	udpEntry.2	INTEGER	R

snmp グループ

MIB	OID	SYNTAX	ACCESS
snmpInPkts	snmp.1	Counter	R
snmpOutPkts	snmp.2	Counter	R
snmpInBadVersions	snmp.3	Counter	R
snmpInBadCommunityNames	snmp.4	Counter	R
snmpInBadCommunityUses	snmp.5	Counter	R
snmpInASNParseErrs	snmp.6	Counter	R
snmpInTooBigs	snmp.8	Counter	R
snmpInNoSuchNames	snmp.9	Counter	R
snmpInBadValues	snmp.10	Counter	R
snmpInReadOnlys	snmp.11	Counter	R
snmpInGenErrs	snmp.12	Counter	R
snmpInTotalReqVars	snmp.13	Counter	R
snmpInTotalSetVars	snmp.14	Counter	R
snmpInGetRequests	snmp.15	Counter	R
snmpInGetNexts	snmp.16	Counter	R
snmpInSetRequests	snmp.17	Counter	R
snmpInGetResponses	snmp.18	Counter	R
snmpInTraps	snmp.19	Counter	R
snmpOutTooBigs	snmp.20	Counter	R
snmpOutNoSuchNames	snmp.21	Counter	R
snmpOutBadValues	snmp.22	Counter	R
snmpOutGenErrs	snmp.24	Counter	R
snmpOutGetRequests	snmp.25	Counter	R
snmpOutGetNexts	snmp.26	Counter	R
snmpOutSetRequests	snmp.27	Counter	R
snmpOutGetResponses	snmp.28	Counter	R
snmpOutTraps	snmp.29	Counter	R
snmpEnableAuthenTraps	snmp.30	INTEGER	R



システムログ情報一覧

モニタのメッセージ

(1) システムダウン

```
init: system down occured.  data is followings:
init:    <elog>
```

【プライオリティ】 LOG_INFO
【意味】 システムダウンが発生したことを示す。
【パラメタの意味】 <elog> ：エラーログ情報

(2) システム起動

```
init: system startup now.
```

【プライオリティ】 LOG_INFO
【意味】 システム起動を示す。

DHCP クライアントのメッセージ

(1) IP アドレス獲得成功

```
dhcpd: Client received DHCPACK [<IP address>] [lan<interface>]
```

【プライオリティ】 LOG_INFO
【意味】 DHCP サーバから DHCPACK を受信し、正常に IP アドレスを受け取った。
【パラメタの意味】 <IP address> ：DHCP サーバから割り当てられた IP アドレス
<interface> ：受信 LAN インタフェース番号

(2) リース更新成功

```
dhcpd: DHCPACK contains different 'your' IP address. reconfigure to new address
```

【プライオリティ】 LOG_INFO
【意味】 リース更新で DHCP サーバから DHCPACK を受信したが、現在使用中の IP アドレスと異なるアドレスが割り当てられたため新しいアドレスに再構成しなおす。
【パラメタの意味】 なし

(3) リース更新失敗 1

```
dhcpd: Received DHCPNAK(RENEWING). lan<interface> go to INIT state
```

【プライオリティ】 LOG_INFO
【意味】 リース更新中（RENEWING 状態）に DHCP サーバから DHCPNAK を受信したため、INIT 状態に遷移し LAN インタフェースを再初期化する。
【パラメタの意味】 <interface> ：LAN インタフェース番号

付録

(4) リース更新失敗２

```
dhcpd: Received DHCPNAK(REBINDING). lan<interface> go to INIT state
```

【プライオリティ】　LOG_INFO
【意味】　リース更新中(REBINDING状態)にDHCPサーバからDHCPNAKを受信したため、INIT 状態に遷移し LAN インタフェースを再初期化する。
【パラメタの意味】　<interface>　: LAN インタフェース番号

(5) リース期間満了

```
dhcpc: The lease time expired. [lan<interface>]
```

【プライオリティ】　LOG_INFO
【意味】　リース期間が満了した。
【パラメタの意味】　<interface>　: LAN インタフェース番号

ftpd のメッセージ

(1) ログイン成功

```
ftpd: login <user> from <address>
```

【プライオリティ】　LOG_INFO
【意味】　ftpd へのログイン成功。
【パラメタの意味】　<user>　: ログインユーザ名
<address>　: クライアントの IP アドレス

(2) ログイン失敗(認証エラー)

```
ftpd: <user> login incorrect from <address>
```

【プライオリティ】　LOG_INFO
【意味】　ftpd へのログイン失敗。
無効なユーザ名またはパスワード誤りである。
【パラメタの意味】　<user>　: ログインユーザ名
<address>　: クライアントの IP アドレス

(3) ファイル蓄積完了

```
ftpd: <filename> Write complete
```

【プライオリティ】　LOG_INFO
【意味】　ファイル蓄積（クライアントからの put）により ROM が上書きされたことを示す。
【パラメタの意味】　<filename>　: 上書きされたファイル名

セキュリティメッセージ

（1）ProxyDNSによるDNS要求破棄

```
proxydns: rejected by <no> : QNAME [<type>:<qname>] from <ipaddr>
```

【プライオリティ】 LOG_NOTICE

【意味】 ProxyDNS において、破棄指定により破棄されたことを示す。

【パラメタの意味】

<no>	: reject を行った proxydns 命令の定義番号。 （注） 画面上の番号ではなく、コマンドライン上の番号。
<type>	: 問い合わせタイプ。
<qname>	: 問い合わせホスト
<ipaddr>	: 発信元ホストの IP アドレス。

（2）IPフィルタによるパケット破棄

```
protocol: rejected at filter(<name>.<no>) : <P> <SA>:<SP> -> <DA>:<DP>
```

【プライオリティ】 LOG_NOTICE

【意味】 IP Filter において、破棄指定により破棄されたことを示す。

【パラメタの意味】

<name>	: ネットワーク名（WAN 側の場合） インタフェース名（LAN 側の場合）
<no>	: reject を行った ip filter 命令の定義番号。 （注） 画面上の番号ではなく、コマンドライン上の番号。
<P>	: プロトコル種別（TCP,UDP,ICMP,IP, その他は番号） TCP の SYN パケットの場合は、TCP(S)と出力する。
<SA>	: source IP address
<SP>	: source port （プロトコル種別がTCP またはUDP であった場合）
<DA>	: destination IP address
<DP>	: destination port （プロトコル種別が TCP または UDP であった場合）

（3）NATによるパケット破棄

```
protocol: rejected at NAT(<name>) : <P> <SA>:<SP> -> <DA>:<DP>
```

【プライオリティ】 LOG_NOTICE

【意味】 NAT において、変換テーブルがなかったことにより破棄されたことを示す。

【パラメタの意味】

<name>	: ネットワーク名（WAN 側の場合） インタフェース名（LAN 側の場合）
<P>	: プロトコル種別（TCP,UDP,ICMP,IP, その他は番号） TCP の SYN パケットの場合は、TCP(S)と出力する。
<SA>	: source IP address
<SP>	: source port （プロトコル種別がTCP またはUDP であった場合）
<DA>	: destination IP address
<DP>	: destination port （プロトコル種別が TCP または UDP であった場合）

（4）NAT変換テーブル作成

```
protocol: NAT:table: <P> <SA> -> <DA>:<DP>
```

【プライオリティ】　LOG_NOTICE
【意味】　NAT において、パケット転送に伴い、変換テーブルを作成したことを示す。
【パラメタの意味】　<P>　: プロトコル種別（TCP,UDP,ICMP,IP, その他は番号）
基本 NAT によるテーブル作成の場合は、ALL と表示する。
<SA>　: source IP address
<DA>　: destination IP address
<DP>　: destination port （プロトコル種別が TCP または UDP であった場合）

（5）DHCPサーバのアドレス配布

```
dhcpd: Server allocation <ip_address> to <mac_address>
```

【プライオリティ】　LOG_NOTICE
【意味】　DHCP サーバが DHCP クライアントにアドレスを配布したことを示す。
【パラメタの意味】　<ip_address>　: DHCP クライアントに配布した IP アドレス
<mac_address>　: DHCP クライアントの MAC アドレス

その他のメッセージ

（1）IP アドレス重複

```
enabled: lan <no> has same network/address as lan <other_no>
```

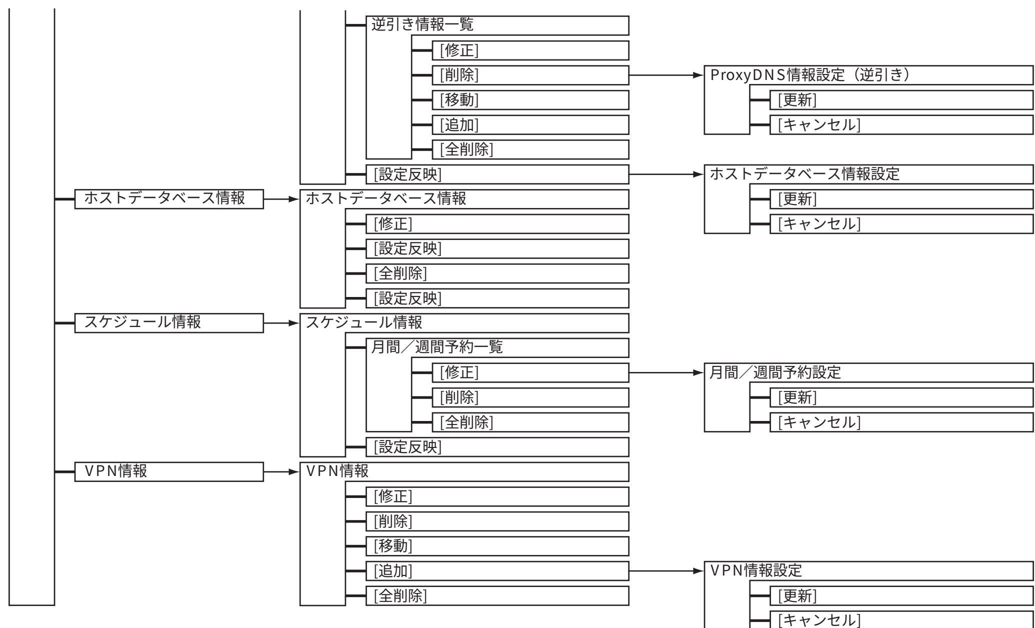
【プライオリティ】　LOG_WARNING
【意味】　<no> と <other_no> の LAN の IP ネットワークアドレス（セカンダリ IP アドレスを含む）が重複していることを示します。
【パラメタの意味】　<no>　: lan 定義番号
<other_no>　: lan 定義番号



「詳細設定」で設定できる項目

- 詳細設定メニュー
  - LAN0情報 → LAN0情報設定
    - IPアドレス
    - セカンダリIPアドレス
    - DHCP機能
      - [修正] → DHCP情報設定
        - DHCP機能
        - [更新]
        - [キャンセル]
    - ダイナミックルーティング機能
    - スタティックルーティング情報一覧
      - [修正]
      - [削除]
      - [追加] → ルーティング情報設定
        - [更新]
        - [キャンセル]
      - [全削除]
    - IPフィルタリング情報一覧
      - [修正]
      - [削除]
      - [移動]
      - [追加] → IPフィルタリング情報設定
        - [LAN情報設定へ戻る]
        - [更新]
        - [キャンセル]
      - [全削除]
    - NAT情報
    - 静的NAT情報一覧
      - [修正]
      - [削除]
      - [追加] → 静的NAT情報追加フォーム
        - [更新]
        - [キャンセル]
      - [全削除]
    - 転送レート
  - LAN1情報 → LAN1情報設定
    - IPアドレス
    - セカンダリIPアドレス
    - DHCP機能
      - [修正] → DHCP情報設定
        - DHCP機能
        - [更新]
        - [キャンセル]
    - ダイナミックルーティング機能
    - スタティックルーティング情報一覧
      - [修正]
      - [削除]
      - [追加] → ルーティング情報設定
        - [更新]
        - [キャンセル]
      - [全削除]
    - IPフィルタリング情報一覧
      - [修正]
      - [削除]
      - [移動]
      - [追加] → IPフィルタリング情報設定
        - [IPフィルタリング情報
        - [更新]
        - [キャンセル]
      - [全削除]
    - NAT情報
    - 静的NAT情報一覧
      - [修正]
      - [削除]
      - [追加] → 静的NAT情報設定
        - [更新]
        - [キャンセル]
      - [全削除]
  - 装置情報 → 装置情報設定
    - ルータ名称
    - タイムサーバ情報
    - システムログ情報
    - ファームウェア更新情報
    - SNMP情報
  - パスワード情報 → パスワード情報設定
  - ProxyDNS情報
URLフィルタ情報 → ProxyDNS情報
    - 順引き情報一覧
      - [修正]
      - [削除] → ProxyDNS情報設定（順引き）
        - [更新]
        - [キャンセル]
      - [移動]
      - [追加]
      - [全削除]

付録


逆引き情報一覧
[修正]
[削除]
ProxyDNS情報設定（逆引き）
[更新]
[キャンセル]
[移動]
[追加]
[全削除]
[設定反映]
ホストデータベース情報設定
[更新]
[キャンセル]
ホストデータベース情報
ホストデータベース情報
[修正]
[設定反映]
[全削除]
[設定反映]
スケジュール情報
スケジュール情報
月間／週間予約一覧
[修正]
月間／週間予約設定
[更新]
[キャンセル]
[削除]
[全削除]
[設定反映]
VPN情報
VPN情報
[修正]
[削除]
[移動]
[追加]
VPN情報設定
[更新]
[キャンセル]
[全削除]



設定内容をメモする

かんたん設定で設定した情報を忘れないように、ここにメモしておきましょう。

プライベートLAN構築かんたん設定

LAN0	IPアドレス	◇DHCPで自動的に取得する		
		◇指定する		
		IPアドレス		.　.　.
		ネットマスク		.　.　.
	転送レート	◇自動認識　◇100Mbps-全二重　◇100Mbps-半二重　◇10Mbps-半二重		
		デフォルトルータ		.　.　.
		DNSサーバアドレス		.　.　.
LAN1		IPアドレス （ご購入時の設定は 192.168.1.1）		.　.　.
		ネットマスク （ご購入時の設定は 255.255.255.0）		.　.　.
		DHCPサーバ	デフォルトルータ広報	.　.　.
			DNSサーバ広報	.　.　.
			ドメイン名広報	.　.　.

セグメント接続／分割かんたん設定

LAN0		IPアドレス （ご購入時の設定は 192.168.0.1）	.　.　.
		ネットマスク （ご購入時の設定は 255.255.255.0）	.　.　.
	転送レート	◇自動認識　◇100Mbps-全二重　◇100Mbps-半二重　◇10Mbps-半二重	
LAN1		IPアドレス （ご購入時の設定は 192.168.1.1）	.　.　.
		ネットマスク （ご購入時の設定は 255.255.255.0）	.　.　.



索引

英数字

付録

あ

か

さ

た

な

は

ま

ら

NetVehicle-L10 取扱説明書
P3NK-E082-04
発行日　　2002年8月
発行責任　富士通株式会社

Printed in Japan